数理科学概論

阪　井　　章

目 次

第1章　代数系

1.1　集合と写像

集合 set とは、ある一定の要件を備えたものの集まりである．集合に属するものを, その集合の**元（または要素) element** という．　a が集合 S の元であることを、記号で

$$a \in S$$

で表す．　ここでは，集合を表す記号として

$$\{x|\cdots\} \qquad \text{または} \qquad \{x:\cdots\}$$

を用いる．S が有限集合であるとき，その元の個数を $|S|$ で表す．　集合 A の元がすべて集合 B の元であるとき、A は B の**部分集合 subset** であるとい,

$$A \subset B$$

とかく．$A \subset B$ と $B \subset A$ が同時に成り立つとき、A と B は一致する．すなわち $A = B$ である．

2つの集合 A , B の両方に属するものの集合を A と B の**共通集合 intersection** といい、$A \cap B$ で表す．　また A か B のいずれかに属するものの集合を A と B の**合併集合 union**（または**和集合**）といい、$A \cup B$ で表す．A に属するが、B には属さないものの集合を $A\backslash B$ とかく：

$$A\backslash B = \{a|a \in A, a \notin B\}$$

元を持たない集合というものを考えると便利である．これを**空集合 empty set** といい、$\emptyset$ で表す．たとえば、A と B が共通部分をもたないとき、A と B は**互いに素である**というが，このことは　$A \cap B = \emptyset$ と書ける．

特定の1つの集合 E の部分集合だけを扱う場合には、補集合というものを考えることがある．　$A \subset E$ に対して $E\backslash A$ を (E における）A の**補集合**といい、A^c で表す．

A の元と B の元を組にしたものの集合：

$$A \times B = \{(a, b)|a \in A, b \in B\}$$

を A と B の**直積 direct product** という.

集合 A の任意の元 x に対して B の 1 つの元 y を対応させる規則が与えられたとき、この規則を A から B （の中）への**写像 mapping, map** という.

$$y = f(x), \qquad f : A \longrightarrow B \qquad x \mapsto y$$

などの記号で表す.

B の集合

$$\{y \in B | \exists x; y = f(x)\}$$

を f の**像 image** または**値域**といい, $f(A)$ または Imf で表す. また, B の部分集合 S に対して, A の集合

$$\{x \in A | f(x) \in S\}$$

を S の f による**逆像 inverse image** といい、 $f^{-1}(S)$ で表す.
とくに f が 1 対 1 対応であるとき，すなわち

$$f(x) = f(y) \Longrightarrow x = y$$

が成り立つとき、f を**単射 injection** という. このとき, すべての $y \in f(A)$ に対して $y = f(x)$ を満たす $x \in A$ がただ 1 つに定まり, y を x に写す写像が定義される. これを f の**逆写像 inverse map** といい f^{-1} で表す. またこのとき, $f^{-1}(S)$ は f^{-1} による S の像になっている.（f^{-1} が定義されなくても, 逆像 $f^{-1}(S)$ は定義されることに注意.）
写像 $f : A \longrightarrow B$ において $f(A) = B$ が成り立つとき, f は A から B の**上への写像**である、または f は**全射 surjeion** であるという.
$B = A$ のとき, 写像 $f : A \longrightarrow A$ を**変換 transformation** ともいう. もし f が全単射であるときには逆写像 f^{-1} を**逆変換**という.
集合 A から 集合 $\{0, 1\}$ への写像 f に対して,

$$S = \{x \in A : f(x) = 1\}$$

は A の 1 つの部分集合である. また，任意の部分集合 S はこの形で表される. A の元 x が S に含まれるときには，$f(x) = 1$，そうでないときには $f(x) = 0$ とすればよい. この f を S の**特性関数 characteristing function** という. A の部分集合と特性関数は 1 対 1 に対応する. とくに，A が大きさ m の有限集合であるとき,A の部分集合の個数は，特性関数の個数 2^m に等しい. 一般に, A の部分集合全部の集合を 2^A で表す.

1.2 数の集合

1.2.1 実数

自然数 natural numbeer　1，2, . . .　全部の集合を $\boldsymbol{N}$ で表す.
整数 integer 全部の集合を $\boldsymbol{Z}$ で表す.

有理数 rational number 全部の集合は $\boldsymbol{Q}$ で表す.
実数 real mumber 全部の集合は $\boldsymbol{R}$ で表す.

自然数 n に関する命題 $P(n)$ について,
［1］$P(1)$ は正しい
［2］すべての自然数 k について, $P(k)$ が正しいことを仮定すれば $P(k+1)$ が正しい
が証明されたとする. このとき, すべての自然数 n について $P(n)$ が成立する. これを**数学的帰納法 mathematical induction** という.

$\boldsymbol{R}$ の中では**四則算法 four arithmetic opertons** が定義される. すなわち、

$$a, b \in \boldsymbol{R} \Longrightarrow a+b \in \boldsymbol{R}, \quad a-b \in \boldsymbol{R}, \quad ab \in \boldsymbol{R}, \quad a/b \in \boldsymbol{R}$$

が成り立つ. $\boldsymbol{Q}$ についても同じ事が成り立つ. $\boldsymbol{Z}$ の中では算法

$$a, b \in \boldsymbol{Z} \Longrightarrow a+b \in \boldsymbol{Z}, \quad a-b \in \boldsymbol{Z}, \quad ab \in \boldsymbol{Z}$$

だけが成り立つ. また、$\boldsymbol{N}$ の中では算法

$$a, b \in \boldsymbol{N} \Longrightarrow a+b \in \boldsymbol{N}, ab \in \boldsymbol{N}$$

だけが成り立つ.

また, すべての $a, b \in \boldsymbol{R}$ に対して, **大小関係**

$$a < b, \quad a > b, \quad a = b$$

のうちいずれかが成り立つ. さらに大小関係と算法の間の関係

$$a > b \Longrightarrow a + c > b + c$$

$$a > b,\ c > 0 \implies ac > bc$$

が成り立つ. $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$はいずれも、R の部分集合であるから、同じ大小関係が成立する.

$\boldsymbol{R}$ においては次のことが成り立つ

アルキメデスの公理 $0 < a < b$ のとき, $b < na$ を満たす自然数 n が存在する.
これまでのことは、$\boldsymbol{R}$ でも $\boldsymbol{Q}$ でも同じように成り立つ. $\boldsymbol{R}$ を $\boldsymbol{Q}$ と分けるのは次の性質である.

Cantor の公理 $\boldsymbol{R}$ の 2 つの数列 $a_n,\ b_n$ が

$$a_n \leqq a_{n+1},\ b_n \geqq b_{n+1},\ a_n \leqq b_n \quad \text{かつ} \quad \lim(b_n - a_n) = 0$$

ならば、

$$\lim a_n = \lim b_n = c$$

となる実数 c が存在する.

これは次の性質と同等である.　$\boldsymbol{R}$ の分割 $[A, B]$ というのは、

$$x \in A, y \in B \Longrightarrow x < y, \quad A \cup B = \boldsymbol{R},\ A \cap B = \emptyset$$

を満たす 2 つの集合 A, B の組である.

Dedekind の公理　$\boldsymbol{R}$ の任意の分割 $[A, B]$ に対して、A の最大数または B の最少数が存在する.

これらの公理は連続性の公理ともよばれる.

1.2.2　複素数

$S = \boldsymbol{R} \times \boldsymbol{R}$ とする. すなわち S は, 2 つの実数の組

$$(a, b)$$

全部の集合である.

$$(a, b) = (a', b') \quad \Longleftrightarrow \quad a = a', b = b'$$

と約束していることに注意する. この S に 2 つの演算, 積と和を次のように定義する：

和　：　$(a, b) + (a', b') = (a + a', b + b')$

積　：　$(a, b)(a', b') = (aa' - bb', ab' + a'b)$

これで四則演算が定義される. このとき, S を**複素数体 complex number field** といい, $\boldsymbol{C}$ で表す. $\boldsymbol{C}$ の元を**複素数 complex number** という.

S の部分集合

$$S_0 = \{(a, 0) \in S\}$$

を考える. 対応

$$a \to (a, 0)$$

は $\boldsymbol{R}$ と S_0 の 1 対 1 対応である. このとき, $\boldsymbol{R}$ の演算は S_0 の演算に対応する. したがって, S_0 は $\boldsymbol{R}$ と同じものと見なす. その元 $(a, 0)$ を単に a で表すことにする. これで $\boldsymbol{R} \subset \boldsymbol{C}$ が成り立つことになる. λ が実数であるとすると

$$\lambda(a, b) = (\lambda, 0)(a, b) = (\lambda a - b0, 0a + \lambda b) = (\lambda a, \lambda b)$$

が成り立つ．これはベクトルのスカラー倍である．すなわち，$\boldsymbol{C}$ は平面ベクトル空間 $\boldsymbol{R}^2$ の構造をもっている．

つぎに，$(0,1)$ を i で表す．すると，

$$(0,1)^2 = (0,1)(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0) = -1$$

であるから，$i^2 = -1$ である．また

$$a + ib = (a,0) + (0,1)(b,0) = (a,0) + (0,b) = (a,b)$$

が成り立つので．複素数 (a,b) を $a+ib$ と書くことができる．これで複素数の定義が済んだ．

$$z = a + ib, \qquad a, b \in \boldsymbol{R}$$

において，a を z の**実数部分 real part**（または実部），b を**虚数部分 imaginary part**（または虚部）といい，

$$a = Rez, \quad b = Imz$$

で表す．$Imz = 0$ ならば z は実数である．$Imz \neq 0$ のとき z を**虚数 imaginary number** という．また

$$|z| = \sqrt{a^2 + b^2}$$

を z の**絶対値 absolute value** という．

$$|z_1 z_2| = |z_1||z_2| \qquad |z_1 + z_2| \leqq |z_1| + |z_2|$$

が成り立つ．また

$$\overline{z} = a - ib$$

を z の**共役複素数 conjugate complex number** という．$\overline{z} = z$ ということは z が実数ということである．

$$z\overline{z} = |z|^2, \quad \overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}, \quad \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$$

などが成り立つ．

$\boldsymbol{C}$ では大小関係を考えない． 算法との関係がうまくいかないからである． すなわち

定理 1.2.1 $\boldsymbol{C}$ においては
(1)$a > b \Longrightarrow a + c > b + c$
(2)$a > b, c > 0 \Longrightarrow ac > bc$
が成り立つような大小関係は存在しない．

次の定理は基本的である．

定理 1.2.2 (de Moivre の公式)

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta, \quad n \in \boldsymbol{Z}$$

実数 x に対して

$$e^{ix} = \cos x + i\sin x$$

とおく. これを**オイラー (Euler) の式**という.

$$|e^{ix}| = 1, e^{-ix} = \overline{e^{ix}} = (e^{ix})^{-1}, e^{2k\pi i} = 1 \ (k \in \boldsymbol{Z})$$

が成り立つ. de Moivre の公式は、オイラーの式を用いれば次のように書ける.

$$(e^{i\theta})^n = e^{in\theta}, \quad n \in \boldsymbol{Z}$$

実数を直線上の点として表現するように、複素数を平面上の点として表すと便利である. x、y 平面の点 (x, y) と複素数 $x + iy$ を同一視したとき, この平面を**複素平面 complex plane**（または**ガウス平面**）という. このとき x 軸の点には実数が、また、y 軸の点には純虚数が対応するので、それぞれ**実軸、虚軸**という.
複素平面の点　$z = x + iy$ に対して，原点 0 と z との距離を r とし, z を表すベクトルと実軸の正の向きとのなす角を　θ とするとき,

$$z = r\cos\theta + ir\sin\theta = re^{i\theta}$$

と書ける. この θ を z の**偏角 argument** という. 偏角は 1 つに定まらない.　θ が z の偏角であれば, $\theta + 2k\pi$ (k は整数）も同じ z の偏角である. z の偏角を $\arg z$ で表す. 2π の整数倍を無視すれば次の等式が成り立つ.

$$arg(z_1 z_2) = arg z_1 + arg z_2$$

$|z| = 1$ 満たす z の集合は, 複素平面内の単位円
を表す. 方程式 $z^n = 1$ の解は

$$z = e^{i2k\pi/n}, \qquad k = 0, 1, ..n-1$$

となるが, これらの複素数を表す点は, 単位円 $|z| = 1$ を n 等分する点である.

1.2.3 代数学の基本定理 Fundamental theorem of algebra

定理 1.2.3 n次の代数方程式

$$a_n z^n + \cdots + a_1 z + a_0 = 0 \quad \text{は } n \text{ 個の (複素数) 解を持つ}$$

いいかえると

$$a_n z^n + \cdots + a_1 z + a_0 = a_n(z-\alpha_1)\cdots(z-\alpha_n), \quad \alpha_k \in \boldsymbol{C}$$

と書けるということである.

1.2.4 整数の整除

この節では、数はすべて整数とする.

定理 1.2.4 $0 < a < b$ とするとき

$$b = aq + r, \qquad (0 \leqq r < a)$$

を満たす自然数 q, r が定まる.

(証明) $aq \leqq b < a(q+1)$ が成り立つように自然数 q 定めることができる. $r = b - aq$ とおけば, $0 \leqq r < a$ が成り立つ. いま

$$b = aq + r = aq' + r' \quad (0 \leqq r, r' < a)$$

であるとすれば, $a(q-q') = r' - r$ である. $-a < r' - r < a$ であるから, $-1 < q - q' < 1$ となるが, $q - q'$ は整数であるから, $q' = q, r' = r$. □

$a, b \neq 0$ に対して $a = bc$ が成り立つとき、b は a を**割る（整除する）**といい、

$$b|a$$

とかく. また、このとき、b は a の**約数**、a は b の**倍数**という
$a_1, .., a_n$ に対して、$m|a_i, i = 1, .., n$ であるとき、m を $a_1, .., a_n$ の**公約数 common divisor** という. $a_1, .., a_n$ の公約数のうちで最大の正数を $a_1, .., a_n$ の**最大公約数 greatest common divisor** といい、$GCD(a_1, .., a_n)$ または $(a_1, .., a_n)$ で表す. $(a_1, .., a_n) = 1$ であるとき、$a_1, .., a_n$ は**互いに素**であるという.
$a_1, .., a_n$ に対して、$a_i|m, i = 1, .., n$ であるとき、m を $a_1, .., a_n$ の**公倍数 common multiplier** という. $a_1, .., a_n$ の公倍数のうちで最小の正数を $a_1, .., a_n$ の**最小公倍数 least**

common divisor といい、$LCM(a_1,..,a_n)$ で表す.

定理 1.2.5　$d=(a_1,..,a_n)$　のとき

$$x_1a_1+\cdots x_na_n=d$$

を満たす $x_1,..,x_n$ が存在する.

(証明) $M=\{x_1a_1+\cdots+x_na_n\}$ とおく.　M に属する整数のうち正のものの最小値を d とすれば $d=(a_1,..,a_n)$ となることを示せばよい.

$d\in M$ であるから $d=x_1'a_1+\cdots+x_n'a_n$ とかける. d の倍数は M に属する. 任意の M の数 $b=x_1a_1+\cdots x_na_n$ に対して　$b=qd+r,(0\leqq r<d)$ となる q,r をとると $r=\sum_{i=1}^{n}(x_i-qx_i')a_i\in M$ となるが　d は最小の正数であるから $r=0,b=qd$ を得る. すなわち　M は d の倍数全部の集合と一致する. 明かに $a_k\in M,k=1,..n$ であるから, $d|a_i,i=1,..n$ が得られる.
m を $a_1,..,a_n$ の任意の公約数とすると, $a_i=k_im,i=1,..,n$ として

$$d=x_1'k_1m+\cdots x_n'k_nm=(x_1'k_1+\cdots+x_n'k_n)m$$

となるから $m|d$, したがって d は　$a_1,..,a_n$ の最大公約数である. □

系 1　$(a_1,..,a_n)=1$ であるための必要十分条件は

$$x_1a_1+\cdots x_na_n=1$$

を満たす $x_1,..,x_n$ が存在することである

系 2　$(a,b)=1,(a,c)=1 \quad\Longrightarrow\quad (a,bc)=1.$
(証明) $ax_1+bx_2=1,ay_1+cy_2=1$ として, これらを乗じて

$$a(ax_1y_1+cx_1y_2+bx_2y_1)+bcx_2y_2=1 \qquad \square$$

整数 p が 1 と p 以外に約数をもたないとき, p を**素数 prime number** という.

系 3　p,q,q' は素数で, $p\neq q,p\neq q'$ のとき, $(p,q^rq'^s)=1$
(証明) $(p,q)=1$ より $(p,q^2)=1$. くり返して $(p,q^r)=1$. 同様にして, $(p,q')=1$ より $(p,q'^s)=1$. ゆえに, $(p,q^rq'^s)=1$ $\square$

系 4 p が素数のとき，p の倍数でない任意の整数 a に対して，整数 b が存在して

$$ab = kp + 1 \quad (k \text{ は整数})$$

定理 1.2.6 すべての整数は素因数の積に (順序を除けば) 一意的に表される.

(証明) $a = p_1^{r_1} \cdots p_n^{r_n} = q_1^{s_1} \cdots q_m^{s_m}$ とする. もし $q_1^{s_1}, .., q_m^{s_m}$ がすべて p_1 と異なるとすれば $(p_1, q_1^{s_1} \cdots q_m^{s_m}) = 1$ すなわち $(p_1, a) = 1$ となって矛盾する. ゆえに, p_1 は $q_1^{s_1}, .., q_m^{s_m}$ のうちのどれかと等しい. (必要なら番号を付け替えて) $p_1 = q_1$ とする. a/p_1 について同じ議論を行う. これを繰り返して $n = m, p_i = q_i, r_i = s_i, i = 1, .., n$ を得る. □

補題 $(a + kb, b) = (a, b)$
(証明) $(a, b) = d$ とすると $a = da', b = db', (a', b') = 1$. c が $a' + kb'$ と b' の約数とすると, $a' + bk' = c\alpha, b' = c\beta$. ゆえに, $a' == c\alpha - kb' = c\alpha - kc\beta = c(\alpha - k\beta)$. $(a', b') = 1$ より $c = 1$. すなわち $(a' + kb', b') = 1, (a + kb, b) = d$ □.

定理 1.2.7 (Euclid の互除法) (a, b) の求め方：
$a = q_0 b + r_1, 0 \leqq r_1 < b; b = q_1 r_1 + r_2; r_1 = q_2 r_2 + r_3; \cdots; r_{n+1} = q r_n \implies r_n = (a, b)$

(証明)
$$\begin{aligned}(a, b) &= (a - q_0 b, b) = (r_1, b) \\ &= (r_1, b - q_1 r_1) = (r_1, r_2) \\ &= (r_1 - q_2 r_2, r_2) = (r_2, r_3) \\ &\quad \cdots \\ &= (r_n, r_{n-1}) = r_n. \quad \square\end{aligned}$$

特定の 0 でない整数 n を 1 つ固定する. 2 つの整数 a, b は, $a - b$ が n で割り切れるとき, n **を法として合同**であるといい,

$$a \equiv b \pmod{n}$$

とかく. これは次の性質をもっている. ($\mathrm{mod}\ n$ は以下省略して書く).
(1) $a \equiv a$
(2) $a \equiv b, b \equiv c \implies a \equiv c$
(3) $a \equiv b, b \equiv a \implies a = b$

n を法として合同であるということは, n で割ったときの余りが等しいということである. a が n と同値であるということは, a が n の整数倍ということである. 余りは

$$o,\ 1,\ 2, \ldots,\ n - 1$$

の n 個あるから，合同なものを 1 つの組にすると，すべての整数は "n" 個の組に分けられることになる．

定理 1.1.5 の系 4 は次のようにいいかえられる．

定理 1.2.8 p が素数であるとき，$a \not\equiv 0 \pmod{p}$ を満たす任意の整数 a に対して 整数 b を選んで次の式が成り立つようにできる．

$$ab \equiv 1 \pmod{p}$$

1.3　関係 relation

(1) 順序関係

自然数の集合 $\boldsymbol{N}$ において 2 つの関係を考えてみよう．

最初のものは，大小関係である．　任意の 2 つの自然数 a と b について

$$a < b, \qquad a = b, \qquad a > b$$

の 3 つの関係のうちどれか 1 つ（1 つだけ）が成立する．　$a < b$ または $a = b$ が成り立つとき, $a \leq b$ と書かれるが, この関係について次のことが成り立つ：

(1) $a \leq a$

(2) $a \leq b, b \leq c \Longrightarrow a \leq c$

(3) $a \leq b, b \leq a \Longrightarrow a = b$

自然数の整除関係 $a|b$ については、次のことが成り立つ：

(1) $a|a$

(2) $a|b, b|c \Longrightarrow a|c$

(3) $a|b, b|a \Longrightarrow a = b$

これら 2 つの関係を aRb であらわすことにすると,

(反射律)　aRa

(推移律)　$aRb, bRc \Longrightarrow aRc$

(反対称律)　$aRb, bRa \Longrightarrow a = b$

を満たすことになる．上の 2 つの関係で違うところは, 順序関係は 任意の 2 つの自然数に対して考えられるのに対して, 整除関係はそうでないことである．$a|b$ が成り立つような順序対 (a, b) の集合を G で表す. 整除という関係を考えるということは $\boldsymbol{N} \times \boldsymbol{N}$ の部分集合 G を考えるということである．　整除関係では，G は $\boldsymbol{N} \times \boldsymbol{N}$ の真部分集合であ

るが, $\boldsymbol{N}$ の大小関係では，G は $\boldsymbol{N} \times \boldsymbol{N}$ に一致する.

一般に, 集合 S に対して, $S \times S$ の部分集合 G を, S の **(2 項) 関係 relation** といい, (a, b) が G に属することを aRb で表す. 関係 R が上の 3 条件を満たすとき, これを**順序関係 order relation** という. 順序関係は普通 $\leqq$ で表される.
集合 S に順序関係が定義されているとする.

$$a \leqq b \qquad \text{かつ} \qquad a \neq b$$

のとき, $a < b$ とかく. S の元 a と部分集合 T に対して

$$\forall x \in T, \quad x \leqq a$$

が成り立つとき，a は T の **上界 upper bound** であるという. 上界を持つ集合は上に有界であるという. T に属する T の上界があれば, それを T の **最大元 maxmum** という. 順序を逆にして, 下に有界な集合と下界, 最小元 infimum が定義される. 集合 S の上界全部の集合の最小元があれば, それを S の**上限 supremum** という. 順序を逆にすれば S の**下限 infimum** のが定義が得られる. 実数の集合 S が上に (下に) 有界であれば，必ず上限 (下限) を持つ.

順序集合 L の 2 つの元 a, b の上限, 下限が存在するとき，これを

$$a \cup b, a \cap b$$

で表す.

(2) 同値関係と商集合

集合 S の関係 R が
(反射律) aRa
(推移律) $aRb, bRc \Longrightarrow aRc$
（対称律） $aRb, \Longrightarrow bRa$
を満たしているとき, 関係 R は**同値関係 equivalece relation** と呼ばれる. $S \times S$ の点 (a, b) が関係 R を定義する部分集合 G に属するとき, a と b は **同値である equivalent** という, a と b が同値であるということを $a \sim b$ とか $a \equiv b$ で表すことが多い.

集合 S において定義された関係 $\sim$ が同値関係であるとき，任意の元 a と同値な元全部の集合を a の**同値類 equvalence class** といい，$[a]$ で表す. すなわち

$$[a] = \{b \in S | b \sim a\}$$

同値類は次の性質を持つ
(1) $a \in [a]$

(2)　$[a] \cap [b] \neq \emptyset \Longrightarrow [a] = [b]$

このことから, S は互いに共通部分を持たない同値類の和集合として表されることがわかる. S の同値類の集合を $S/\sim$ で表し, $\sim$ による S の**商集合**という.

例 1　0 でない整数 n を 1 つ固定する. 2 つの整数 a, b について

$$n|(a-b) \qquad (a-b \text{ が } n \text{ で割り切れる})$$

が成り立つとき, $a \sim b$ と定義すると, 第 1.1.4 節で述べたようにこれは $\boldsymbol{Z}$ の同値関係になる.　この同値関係による商集合 $\boldsymbol{Z}/\sim$ を $\boldsymbol{Z}_n$ で表す.

例 2　n 次正方行列の集合を M_n とする. $A, B \in M_n$ に対して, 正則行列 P があって

$$B = P^{-1}AP$$

が成り立つとき, $A \sim B$ と定義すると, これは M_n の同値関係である.

例 3　0 でない整数の集合を $\boldsymbol{Z}^*$ で表す. 直積集合 $\boldsymbol{Z} \times \boldsymbol{Z}^*$ の 2 つの要素 (a, b), (a', b') が

$$ab' - a'b = 0$$

を満たしているとき, $(a, b) \sim (a', b')$ と書くことにすると 関係 $\sim$ は同値関係である. (この同値関係による商集合 $\boldsymbol{Z} \times \boldsymbol{Z}^*/\sim$ を $Q(\boldsymbol{Z})$ と書く.　後で述べるように, $Q(\boldsymbol{Z})$ は有理数体 $\boldsymbol{Q}$ と同じものと考えられる.

1.4 代数系

1.4.1 算法

集合 S の任意の２つの元 a,b に対して, S の１つの元が対応する規則が与えられているとする. いいかえると、写像

$$F : S \times S \longrightarrow S$$

が与えられているとする. このとき, F を S の**算法**または**演算 operation** という. ここでは $F((a,b))$ を $a \circ b$ と表すことにする. 集合 S と算法 $\circ$ を組にして, $(S,\circ)$ （または単に S）を**代数系**という.

算法 $\circ$ に対して，規則

$$(a \circ b) \circ c = a \circ (b \circ c)$$

を**結合則 associative law** という．ふつう算法といえば結合則を満たしているものである.

また，算法 $\circ$ に対して，規則

$$a \circ b = b \circ a$$

を**交換則 commutative law** という．算法は交換則を満たしているとは限らないが、これが $S \times S$ のすべての元に対して成り立つときは、この算法 (またはこの代数系) は**可換 commutative** であるという.

例 1 $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{R}$, $\boldsymbol{Q}$, $\boldsymbol{C}$ において, 通常の和および積は可換な算法である.

例 2 n 次数ベクトル全部の集合 $\boldsymbol{R}^n$ においては, 和が定義されるが，これは可換である.（この他にスカラー倍が定義される (後述).）

例 3 $m \times n$ 行列全部の集合 においては, 和は可換である.

例 4 $n \times n$ 行列全部の集合においては，積が定義されるが可換ではない.

例 5 n 次の置換全部の集合 S_n (後述）においては， 積が定義されるが, 可換ではない.

例 6 区間 I で連続な関数全部の集合 $C(I)$ においては

$$(f+g)(x) = f(x) + g(x), \qquad (fg)(x) = f(x)g(x)$$

によって和 $f+g$ と積 fg が定義されるがいずれも可換である.

例 7 区間 I と 点 $x_0 \in I$ に対して，$C(I)$ の部分集合

$$J(I) = \{f \in C(I) : f(x_0) = 0\}$$

では，和および積が定義される．S の元 e が

$$\text{全ての元 } x \in S \text{ に対して} \quad e \circ x = x \circ e = x$$

満たしているとき, e をこの算法の**単位元 unit** という．例 1 の $\boldsymbol{Z}, \boldsymbol{R}, \boldsymbol{Q}, \boldsymbol{C}$ では, 和の単位元は 0 であり, 積の単位元は 1 である．例 2 では単位元は零ベクトルである．例 3 では和の単位元は零行列で、例 4 では積の単位元は単位行列である．例 5 では単位元は恒等置換である． 例 6 では和の単位元は定数関数 0 で, 積の単位元は定数関数 1 である． 一般に単位元は存在するとは限らない．例えば $\boldsymbol{N}$ では, 積の単位元は 1 であるが, 和の単位元はない（0 は属していない）．例 7 では，和の単位元は 定数関数 0 であるが，積の単位元はない．単位元は, もし存在するならばただ 1 つである．

S の算法 $\circ$ が単位元 e をもつ場合, S の元 a に対して S の元 a' があって,

$$a \circ a' = a' \circ a = e$$

が成り立つならば, a は**逆元 inverse element** を持つといい，a' を a^{-1} で表す．逆元はいつも存在するとは限らない．もし存在するならばただ 1 つである．

算法を表す記号としては, 実数の算法における積の記号 $a \cdot b$ または和の記号 $a + b$ がよく使われる．

1.4.2 準同型写像

算法 $\circ$ をもつ代数系 S から算法 $\bullet$ をもつ代数系 S' への写像 f が

$$f(a \circ b) = f(a) \bullet f(b)$$

を満たすとき，f を S から S' への**準同型写像 homomorphism** という．とくに, f が全写でかつ単写であるとき, これを**同型写像 isomorphism** といい, $(S, \circ)$ と $(S', \bullet)$ は**同型であるとか同じ構造をもつ**という．

,

1.4.3 直積代数系

算法 $\circ$ をもつ代数系 A と算法 $\bullet$ をもつ代数系 B に対して, 直積集合 $A \times B$ において算法 $\circ \times \bullet$ を

$$(a, b) \circ \times \bullet (a', b) = (a \circ b, a' \bullet b')$$

によって定義すると $A \times B$ は 1 つの代数系となる．

1.4.4 商代数系

算法 $\circ$ をもつ集合 S において, 同値関係 $\sim$ が定義されているとする. もし

$$a \sim a',\ \ b \sim b' \Longrightarrow a \circ b \sim a' \circ b'$$

が成り立つならば, $\circ$ と $\sim$ は**両立する compatible** という. このとき, 同値類 $[a \circ b]$ は同値類 $[a], [b]$ のそれぞれの代表元の選び方に関係しない. そこで

$$[a] \circ [b] = [a \circ b]$$

と定義すれば, 同値類の集合に算法 $\circ$ が定義される. このようにして S の商集合 $S/\sim$ は代数系となる.

1.2.3 節の例 1, 例 3 の $\boldsymbol{Z}_n$ と $Q(\boldsymbol{Z})$ は (加法および乗法について) 商代数系となる. とくに, p が素数であるとき, $\boldsymbol{Z}_p$ では 0 でない数は乗法の逆元をもつ (定理 1.1.8). つまり, $\boldsymbol{Z}_p$ では割り算もできるということである.

1.4.5 いろいろな代数系

ここでは, いろいろな代数系の定義だけを述べる.

半群 集合 S が算法 $\circ$ もち, 条件 (結合律)$(a \circ b) \circ c = a \circ (b \circ c)$
を満たすとき, $(S, \circ)$ を**半群 semigroup** という. 可換律を満たす半群を**可換半群**という.

モノイド $(M, \circ)$ が半群で, かつ単位元をもつとき, M を**モノイド monoid** という. 可換律を満たすモノイドを可換モノイドという.

群 モノイド G のすべての元に対して, 逆元が存在するとき, G を**群 group** という. 可換律を満たす群を**可換群**または**アーベル群**という. 群については、算法を ab などの通常の積の記号で表す. 可換群においては, 算法はしばしば加法の記号 $a+b$ を用いる. このとき, G を**加法群**といい, a の逆元は $-a$ で表し, 単位元は 0 で表すのが普通である.

環 集合 R が 2 つの算法：和 $+$ と 積 $\cdot$ をもち, $(R, +)$ が可換群 (加法群) で, $(R, \circ)$ が単位元をもつ可換半群であって, 条件
(分配律) $a \cdot (b+c) a \cdot b + a \cdot c$
$(b+c) \cdot a = b \cdot a + c \cdot a$
を満たしているとき, $(R, +, \cdot)$ (または単に R) を**環 ring** という.
乗法の単位元を持つとは限らないとする定義もあるが, ここでは. 乗法をもつものとする. その単位元を 1 で表す. 積 $a\dot{b}$ は普通 ab で表す.

整域 0 以外の元をもつ可換環 R において

$$ab = 0 \quad \Longrightarrow \quad a = 0 \quad \text{または} \quad b = 0$$

が成り立つとき，R を整域 integral domain という．整数全部の集合 $\boldsymbol{Z}$ は整域である．
例 平面領域 D で正則な関数全部の集合も整域である．(D で連続な関数全部の集合は整域ではない)．

加群 環 A を作用域とする加法群 M を $A-$ **加群 A-module** という．

体 代数系 $(K, +, \cdot)$ において, $(K, +)$ が可換群で，$(K/\{0\}, \cdot)$ が可換群で, 分配法則

$$a(b + c) = ab + ac$$

を満たすとき，$(K, +, \cdot)$ （または単に K）を**体 field** という．積 $a\dot{b}$ は普通 ab で表す．
注意： 体の定義で，積についての可換性を仮定するのが普通である．積について可換でないものを**斜体**という．環の定義では積についての可換性を仮定していないことに注意.

順序体　体 K が順序関係で全順序集合で，さらに条件
(1) $a \leqq b \Longrightarrow a + c \leqq b + c$
(2) $a \leqq b, c > 0 \Longrightarrow ac \leqq bc$
が成り立つとき, K を**順序体**という．$\boldsymbol{R}$ や Q は順序体である．
問　$\boldsymbol{C}$ は順序体でないことを証明せよ

線形空間（ベクトル空間）　体 K と加法群 V と写像

$$F : K \times V \quad \longrightarrow \quad V$$

があるとき, $\lambda \in K$ と $x \in V$ に対して

$$F((\lambda, x)) = \lambda x$$

とかき，これをスカラー倍という．条件
(1) $\lambda(x + y) = \lambda x + \lambda y$
(2) $(\lambda + \mu) = \lambda x + \mu x$
(3) $(\lambda\mu)x = \lambda(\mu x)$
(4) $1x = x$
を満たしているとき, V を K 上の**線形空間 (ベクトル空間) linear space (vector space)** という．

多元環　K 上の線形空間 A において乗法が定義され,

(1) $x(yz) = (xy)z, \quad (x+y)z = xz + yz, \quad x(y+z) = xy + xz, \quad x, y, z \in A$
(2) $\lambda(xy) = x(\lambda y) = (\lambda x)y, \quad x, y \in A,\ \lambda \in K$
を満たすとき, A を K 上の**多元環 algebra** という.

束
順序集合 L において, すべての元 a, b に対して $a \cup b, \quad a \cap b$ が存在するとき，これらは L の算法である．これら算法が可換律と結合律のほか次の条件を満たすとき, $(L, \cup, \cap)$ または L を**束 (Lattice)** という：
（吸収律） $a \cup (a \cap b) = a \cap (a \cup b) = a$
束においては次の等式が成り立つ.
（べき等律）$a \cup a = a, \quad a \cap a = a$

代数系 $(S, \circ)$ の他に集合 Σ があり，Σ の任意の元 a について写像

$$\varphi_a : S \longrightarrow S$$

があって,

$$\varphi_a(x \circ y) = \varphi_a(x) \circ \varphi_a(y),\ x, y \in S$$

を満たすとき，φ_a または a を **作用子**，Σ を**作用域 domain of operator** という．このとき，Σ は S に作用しているという.

K 上の線形空間 V は，K を作用域とする加群である.

注意： 写像 $S \longrightarrow S$ の集合を $\mathrm{trans}(S)$ と書くとき， $a \mapsto \varphi_a$ によって写像

$$\varphi\Sigma \longrightarrow \mathrm{trans}(S)$$

が定義される．これを作用という．また，写像

$$\psi : \Sigma \times S \longrightarrow S$$

のことを作用ということもある．作用を外部演算，S の演算を内部演算ということもある．
$\phi_a(x)$ を ax とも書く

1.4.6 線形空間 linear space

次元 dimension

V を体 K 上の線形空間とする． V の元 $\boldsymbol{a}_1, ..., \boldsymbol{a}_m$ が

$$c_1\boldsymbol{a}_1 + \cdots + c_m\boldsymbol{a}_m = \mathbf{0} \Longrightarrow \quad \mathbf{c_1} = \cdots = \mathbf{c_m} = \mathbf{0}$$

を満たすとき，$\boldsymbol{a}_1, ..., \boldsymbol{a}_m$ は**１次独立 linearly independent** であるという．

線形空間 V の元 $\boldsymbol{a}_1, ..., \boldsymbol{a}_r$ が次の２つの条件を満たしているとき，$\{\boldsymbol{a}_1, ..., \boldsymbol{a}_r\}$ は V の**基底 basis** であるという:

(1) $\boldsymbol{a}_1, ..., \boldsymbol{a}_r$は１次独立である．

(2) すべての$\boldsymbol{z} \in V$ は$\boldsymbol{a}_1, ..., \boldsymbol{a}_r$の１次結合である：

$$\boldsymbol{a} = \lambda_1\boldsymbol{a}_1 + \cdots + \lambda_r\boldsymbol{a}_r$$

１組の基底があれば，無数の基底がある．しかし，基底のベクトルの個数 r は 一定である．この r を V の**次元 dimension** といい, $\dim V$ で表す．基底が存在しない場合は，V は無限次元であるという．

線形写像

線形空間 V から V' への写像 f が

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y), \quad \lambda,\ \mu \in K,\ x,\ y \in V$$

を満たすとき，f は V から V' への**線形写像（１次写像）linear mapping** という．とくに，$V = V'$ のときは，**線形変換（１次変換）**という．

***R*または*C*上の線形空間**

$K = \boldsymbol{R}$ (または $K = \boldsymbol{C}$) の場合，V を**実 (または複素) 線形空間** という．(線形空間は一般ベクトル巣空間空間または抽象ベクトル空間ともよばれる.）V が複素線形空間ならば，V は実線形空間とも考えられる． このとき注意を要することは，１次独立性である．複素１次独立ならば実１次独立である． たとえば，実２次元の空間 R^2 (平面) において，ベクトル $(1, 0)$ と $0, 1)$ は １次独立であるが，平面を複素線形空間 (複素平面) ととしてみると 1 と i は１次従属で，複素平面は １次元である．一般に，V が n 次元複素線形空間ならば，実線形空間としては $2n$ 次元となる．

内積空間

R 上の線形空間 V において，V の任意の２つの元 $\boldsymbol{a}$, $\boldsymbol{b}$ に対して実数 $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ を対応させる規則が与えられていて，次の条件を満たすとき，V は**内積空間**であるといい，$\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ を $\boldsymbol{a}$と$\boldsymbol{b}$ の**内積 inner product** という．

(1) $\langle \boldsymbol{a}, \boldsymbol{a} \rangle$ は負でない実数である

(2) $\langle \boldsymbol{a}, \boldsymbol{a} \rangle = 0 \iff \boldsymbol{a} = \boldsymbol{0}$
(3) $\langle \boldsymbol{b}, \boldsymbol{a} \rangle = \langle \boldsymbol{a}, \boldsymbol{b} \rangle$
(4) $\langle \boldsymbol{a}_1 + \boldsymbol{a}_2, \boldsymbol{b} \rangle = \langle \boldsymbol{a}_1, \boldsymbol{b} \rangle + \langle \boldsymbol{a}_2, \boldsymbol{b} \rangle$
(5) $\langle \lambda \boldsymbol{a}, \boldsymbol{b} \rangle = \lambda \langle \boldsymbol{a}, \boldsymbol{b} \rangle$
このとき
(4') $\boldsymbol{a}, \boldsymbol{b}_1 + \boldsymbol{b}_2 \rangle = \langle \boldsymbol{a}, \boldsymbol{b}_1 \rangle + \langle \boldsymbol{a}, \boldsymbol{b}_2 \rangle$
(5') $\langle \boldsymbol{a}, \lambda \boldsymbol{b} \rangle = \lambda \langle \boldsymbol{a}, \boldsymbol{b} \rangle$
が成り立つ.
C 上の線形空間 V において V の任意の 2 つの元 $\boldsymbol{a}$, $\boldsymbol{b}$ に対して複素数 $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ を対応させる規則が与えられていて，次の条件を満たすとき，V は **(複素) 内積空間**であるといい，$\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ を $\boldsymbol{a}$と$\boldsymbol{b}$ の **(複素) 内積 またはエルミート内積**という.
(1) $\langle \boldsymbol{a}, \boldsymbol{a} \rangle$ は負でない実数である
(2) $\langle \boldsymbol{a}, \boldsymbol{a} \rangle = 0 \iff \boldsymbol{a} = \boldsymbol{0}$
(3) $\langle \boldsymbol{b}, \boldsymbol{a} \rangle = \overline{\langle \boldsymbol{a}, \boldsymbol{b} \rangle}$
(4) $\langle \boldsymbol{a}_1 + \boldsymbol{a}_2, \boldsymbol{b} \rangle = \langle \boldsymbol{a}_1, \boldsymbol{b} \rangle + \langle \boldsymbol{a}_2, \boldsymbol{b} \rangle$
(5) $\langle \lambda \boldsymbol{a}, \boldsymbol{b} \rangle = \lambda \langle \boldsymbol{a}, \boldsymbol{b} \rangle$
違いは条件 (3) である．(4') は同じであるが，(5') は次のようになる.
(5') $\langle \boldsymbol{a}, \lambda \boldsymbol{b} \rangle = \overline{\lambda} \langle \boldsymbol{a}, \boldsymbol{b} \rangle$

内積空間 V において，$\boldsymbol{a} \neq \boldsymbol{0}$, $\boldsymbol{b} \neq \boldsymbol{0}$ で

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \boldsymbol{0}$$

が成り立つとき．$\boldsymbol{a}$と$\boldsymbol{b}$ は**直交する** という.

ノルム空間 C 上の線形空間 V において V の任意の元 $\boldsymbol{a}$ に対して負でない実数 $\| \boldsymbol{a} \|$ を対応させる規則が与えられていて，次の条件を満たすとき，V は**ノルム空間 normed space** であるといい，$\| \boldsymbol{a} \|$ を $\boldsymbol{a}$ の**ノルム norm** という.
(1) $\| \boldsymbol{a} \| = 0 \iff \boldsymbol{a} = \boldsymbol{0}$
(2) $\| \lambda \boldsymbol{a} \| = |\lambda| \, \| \boldsymbol{a} \|$, $\lambda \in \boldsymbol{C}$
(3) $\| \boldsymbol{a} + \boldsymbol{b} \| \leqq \| \boldsymbol{a} \| + \| \boldsymbol{b} \|$

内積空間 V において

$$\| \boldsymbol{a} \| = \sqrt{\langle \boldsymbol{a}, \boldsymbol{a} \rangle}$$

とおく．これによって V はノルム空間となる．このとき，$\| \boldsymbol{a} \|$ を $\boldsymbol{a}$の長さともいい，$|a|$ と書くときもある.

例 1 $\boldsymbol{R}^n$ の次元 n. その部分ベクトル空間 $V = \{ \boldsymbol{x} \in \boldsymbol{R}^n : A\boldsymbol{x} = \boldsymbol{0} \}$ (A は $m \times n$ 行列) の次元は $n - \mathrm{rank} A$.

例 2　$m \times n$ 行列全部の集合.

例 3　I を実数 t のある区間とするとき

$$V = \{f : f(t) \text{は　Iで連続な関数}\}$$

を考える.

$$(f+g)(t) = f(t) + g(t), \qquad (\lambda f)(t) = \lambda f(t)$$

によって，和 $f+g$ およびスカラー倍 λf を定義する．また，零元は I のすべての t について値が 0 である関数とする．また,

$$-f(t) = (-1)f(t)$$

によって $-f$ を定義する．こうすると，V は上の条件をすべて満たし，線形空間となる．この空間を $C(I)$ で表す.

例 4　区間 I で連続で

$$\int_I |f(t)|^2 dt < \infty$$

を満たす関数 $f(t)$ 全部の集合 V．このとき内積を

$$\langle f, g\rangle = \int_I f(t)g(t)dt$$

によって定義することにより，V は内積空間となる.

例 5　区間 I で 1 回連続的微分可能な関数（$f'(t)$ が連続な関数 f）全部の集合　$C^1(I)$
これは $C(I)$ の部分集合で，和，積，零元などは $C(I)$ と同じとする.
同じように

例 6　区間 I で k 回連続的微分可能な関数（$f^{(k)}(t)$ が連続な関数 f）全部の集合　$C^k(I)$

例 7　区間 I で何回でも微分可能な関数全部の集合　$C^\infty(I)$

も定義される.

例 3 - 例 7 はすべて無限次元

例 8　高々 n 次の多項式全部の集合 V
高々 n 次の多項式は

$$p(x) = a_n x^n + \cdots + a_1 x + a_0$$

の形をしている．この多項式と $n+1$ 次数ベクトル $(a_n, \cdots, a_0)$ とが 1 対 1 に対応しており，演算などがそのまま対応しているので，V は，線形空間として，$\boldsymbol{R}^{n+1}$ と同じとみて

よい．$\{1, x, \ldots, x^n\}$ は V の基底であるが，一般に，最高次の係数が 1 に等しい k 次の多項式を $p_k(x)$ とするとき，$\{p_0(x), p_1(x), \ldots, p_n(x)\}$ は V の基底である．

もう一つ重要な例は斉次線形微分方程式の解の空間である．

例 9　$P(t), Q(t)$ が I で連続であるとき

$$V = \{y(t) \in C^2(I) : \frac{d^2y}{dt^2} + P(t)\frac{dy}{dt} + Q(t)y = 0\}$$

V の次元は 2 である．

以上はすべて $\boldsymbol{R}$ 上の線形空間である．対応する $\boldsymbol{C}$ 上の線形空間が考えられる．

1.5　群

群の算法の満たす条件は次の通りである.

$(G_1) a(bc) = (ab)c$

$(G_2) \exists e \in G; ae = ea = a \quad \forall a \in G$

$(G_3) \forall a \in G, \quad \exists a'; aa' = a'a = e$

条件 (G_2), (G_3) は次の条件に置き換えることが出来る：

$(G_2)' \exists e \in G; ea = a \quad \forall a \in G$

$(G_3)' \forall a \in G, \exists a'; a'a = e$

単位元 e はただ一つである. また, a^{-1} は a によってただ一つに定まる.　さらに, 条件

(交換律)　$ab = ba \quad \forall a, b$

が満たされるときは, G は**可換群 commutative group（アーベル群 abelian group）**であるという. このとき, しばしば算法として和の記号 $+$ を用い, G を**加法群 additive group** という. [注意] 後述の加群と混同しないこと！

群 G の元の個数を G の**位数 order** という. 位数が有限の群を**有限群 finite group** という.

群 G の元 a の n 個の積を a^n で表す. さらに,

$$a^0 = e, \qquad a^{-n} = (a^{-1})^n$$

と定義すると，すべての整数 n に対して a^n が定義され，指数法則

$$a^n a^m = a^{n+m}, \qquad (a^n)^m = a^{nm}$$

が成り立つ.

群 G の元が, G の特定の元 a の累乗（べき）であるとき, G を a によって生成される**巡回群 cyclic group** といい, a を G の**生成元**といい，$G =< a >$ で表す. 巡回群はアーベル群である.

G の部分集合 A, B に対して

$$AB = \{ab : a \in A, b \in B\}, \qquad A^{-1} = \{a^{-1}; a \in A\}$$

とおく.

$$(AB)C = A(BC), \qquad (AB)^{-1} = B^{-1}A^{-1}$$

が成り立つ.

とくに，$B = \{b\}, C = \{c\}$ のときには

$$\{b\}A, \qquad A\{b\}, \qquad \{b\}A\{c\}$$

のかわりに

$$bA, \qquad Ab, \qquad bAc$$

とかく.

1.5.1 群の例

例 1 数のつくる群
実数の集合 $\boldsymbol{R}$, 有理数の集合 $\boldsymbol{Q}$, 整数の集合 $\boldsymbol{Z}$, 複素数の集合 $\boldsymbol{C}$ は算法 + に関して群である. $\boldsymbol{N}$ や $\boldsymbol{R}^+$ 群でない.
また $R^* = \boldsymbol{R} \setminus \{0\}$, $\boldsymbol{Q} \setminus \{0\}$, $C^* = \boldsymbol{C} \setminus \{0\}$ は積に関して群である. $\boldsymbol{Z}$ は積に関して群にならない.

例 2 置換群
集合 Ω から Ω の上への 1 対 1 写像を Ω の**変換 transformation** または**置換 permutation** という. Ω のすべての元をそれ自身にうつす写像を恒等置換という. 置換の逆写像を逆置換という. 写像としての合成を積とすれば, これによって, Ω の置換全部の集合は群をつくる. 一般に, Ω の置換の集合 G が群をなしているとき, これを Ω の**変換群**または**置換群**という.
とくに, $\Omega = \{1, 2, .., n\}$ のとき, Ω の置換を n **次の置換**という. n 次の置換のつくる群を n **次対称群 symmetric group** といい, S_n で表す.

例 3 回転群
3 次元ユークリド空間の置換において, 任意の 2 つの点の距離と置換によって写された 2 点の距離が等しいとき, この置換を合同変換という. 定直線を軸とする回転, 定平面に関する対称移動, および, 平行移動は合同変換で, 一般の合同変換はこれら 3 種類の合同変換の合成によって得られる. 合同変換全部の集合は, 群になる. これを**合同変換群**という.
定点 O を通る回転全部の集合は群をつくる. これを**回転群**という. 回転群は次のような有限群を含む. 3 次元空間の中で, 正多角形を考える. この多角形には, 表面と裏面があるとみなして, これを 2 面体ということにする. 頂点の数が n のとき, 正 n 角形という. これは, 裏表のある円板を考えて, その周上を n 等分する点に印を付けたものと考えてもよい. 印が頂点で, 隣り合った印の間の円弧が辺である. 正 n 角形を自分自身に写す回転には次のものがある.
(1) 中心の回りの回転
(2) n が偶数（奇数）のとき, 相対する頂点（頂点と対辺の中点）を結ぶ直線の回りの回転
(3) n が偶数のときは, 相対する辺の中点を結ぶ直線の回りの回転
これらの回転と恒等変換を併せて, 群をつくる. これを 2 面体群という. たとえば, $n = 2$ の場合には, 恒等変換の他に, (1) が 1 個, (2) が 1 個, (3) が 1 個あり, これらは位数 4 の群を作る. この群は $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ と同型である.
正多面体には正 4 面体, 正 6 面体, 正 8 面体, 正 1 2 面体, 正 2 0 面体の 5 種類がある. 中心 O とする回転で, このうちの特定の正多面体を自分自身に写す変換は群をつくる. 正 n 面 体から生じる回転群を正 n 面体群といい, $P(n)$ で表す. これらの群においては, 恒等変換の他に, 次の 4 種類の回転が考えられる (無い場合もある）.

(1) 相対する頂点を結ぶ直線の回りの回転
(2) 相対する面の中心を結ぶ直線の回りの回転
(3) 相対する辺の中点を結ぶ直線の周りの回転
(4) 頂点と相対する面の中心を結ぶ直線の回りの回転
$P(4)$ においては，恒等置換のほかに，(3) が3個，(4) が8個で，計12個あるある．回転は4個の頂点の偶置換を引き起こすが, $|A_4| = 12$ であるから，$P(4) \cong A_4$ である．

$P(6)$ においては，4つの対角線の置換を引き起こす. 恒等置換のほかに, (1) が8個，(2) が9個，(3) が6個で，合計24個．これは $|S_4|$ に等しいから，$P(6) \cong S_4$ である．
$P(20)$ においては，(1) が20個，(2) が24個，(3) が15個で，計60個．これは $|A_5|$ に等しいから, $P(20) \cong A_5$ である．
$P(8)$ の変換は，中に含まれる正6面対の回転を引き起こし，逆に, $P(6)$ の変換は $P(8)$ の変換を引き起こす．したがって, $P(8) \cong P(6)$ である．
同じようにして，$P(12) \cong P(20)$ となる．

例 4　剰余類群

1,2.3 節で述べた $\boldsymbol{Z}_n$ は加法に関して可換群をつくる．これを**剰余類群 residual class group** という．x を含む類を $[x]$ で表すことにすると，零元は $[0]$ であり, $[a]$ の 逆元は $[-a]$ である．
$\boldsymbol{Z}_n$ は位数 n の巡回群である．$\boldsymbol{Z}_n$ の元を代表元によって $\{0, 1, 2, .., n-1\}$ で表すことがある．このとき

$$(n-1) + 1 = 0$$

である．とくに，$\boldsymbol{Z}_2$ は 0 と 1 とからなり，その算法は

$$0 + 1 = 1 + 0 = 1, 1 + 1 = 0$$

である．
$\boldsymbol{Z}_n^* = \boldsymbol{Z}_n \setminus [0]$ は乗法によってモノイドであるが，一般に群にはならない． とくに，n が素数 p であるときは，p と同値でない任意の a に対して

$$ab \sim 1$$

を満たす b が存在する (定理 1.1.5 系 4). したがって，$\boldsymbol{Z}_p$ は群になる．

例 5　行列の群

$m \times n$ 実行列全部の集合 $M(m, n, \boldsymbol{R})$ は加法に関して群をつくる．とくに，$m = n$ のとき，$M(n, n, \boldsymbol{R})$ を $M(n, \boldsymbol{R})$ とかく．
また, n 次実正則行列全部の集合は乗法に関して群をつくる．これを**一般線形群 general linear group** といい, $GL(n, \boldsymbol{R})$ で表す． とくに, 行列式の値が 1 に等しい行列式全部の集合は**特殊線形群 special linear group** といい，$SL(n, \boldsymbol{R})$ で表す．n 次直交行列の

集合は**直交群 orthogonal group** といい $O(n)$ で表す：

$$O(n) = \{P \in GL(n, \boldsymbol{R}) : P^{-1} = {}^tP\}$$

複素行列の場合は $GL(n, \boldsymbol{C}), S(n, \boldsymbol{C})$ とかく. ユニタリー行列の集合は

$$U(n) = \{U \in GL(n, \boldsymbol{C}) : U^{-1} = U^*\}, \qquad (U^* = {}^t\bar{U})$$

である.

例 6　直積（直和）　n 個の群 $G_1, G_2, .., G_n$ の直積集合 $G = G_1 \times \cdots \times G_n$ において $a = (a_1, .., a_n),\ b = (b_1, .., b_n)$　の積を

$$ab = (a_1b_1, ..., a_nb_n)$$

によって定義する. 単位元と逆元を

$$e = (e_1, .., e_n) \qquad a^{-1} = (a_1^{-1}, , , , a_n^{-1})$$

で定義すると, G は群になる. これを $G_1, .., G_n$ の**直積**といい,　$G_1 \otimes \cdots \otimes G_n$ と書く. $G_1, G_2, .., G_n$ が加法群である場合には算法を

$$a + b = (a_1 + b_1, .., a_n + b_n)$$

によって表し, G を $G_1 \oplus \cdots \oplus G_n$ と書いて**直和 direct sum** という.

1.5.2　部分群

群 G の部分集合 H が, G の算法によって群をつくるとき，すなわち

(1)　$a, b \in H \Longrightarrow ab \in H$

(2)　$a \in H \Longrightarrow a^{-1} \in H$

を満たすとき，H を G の**部分群 subgroup** といい，$H < G$ または $G > H$ とかく.

条件 (1),(2) は次の条件と同値である：

(3) $a, b \in H \Longrightarrow ab^{-1} \in H$

すべての $a \in G$ に対して

$$aHa^{-1} = H$$

を満たす部分群 H を**正規部分群 normal subgroup** といい

$$H \lhd G \qquad \text{または} \qquad G \rhd H$$

で表す.　アーベル群の部分群はすべて正規部分群である.

G 自身および $\{e\}$ は G の部分群である.　そのほかの重要な部分群の例を述べる.

例 1　加法群として $\boldsymbol{Z}$ は $\boldsymbol{R}$ の部分群であり，$\boldsymbol{R}$ は $\boldsymbol{C}$ の部分群である．
例 2　加法群 $\boldsymbol{Z}$ において，$a \in \boldsymbol{Z}$ に対して集合

$$< a >= \{ma : m \in \boldsymbol{Z}\}$$

は，$\boldsymbol{Z}$ の部分群である．逆に, $\boldsymbol{Z}$ の部分群 H は，ある $a \in \boldsymbol{Z}$ に対して　$H =< a >$ と書ける．
(後半の証明）$H = \{0\}$ ならば $H =< 0 >$ である．$H \neq \{0\}$ ならば，H に含まれる最小の正数がある．それを a とする．任意の　$x \in H$ に対して

$$x = ma + r, \quad 0 \leqq r < a$$

と書ける．$x, ma \in H$ であるから $r \in H$ であるが，a の定義から　$r = 0$ すなわち $x = ma$ となる．□

例 3　群 G において $a \in G$ に対して，a によって生成される巡回群

$$< a >= \{a^n : n \in \boldsymbol{Z}\}$$

は G の部分群である．対応 $m \to a^m$ によって定義される写像 $Z \to < a >$ は準同型写像であるから，その核　$\{m \in \boldsymbol{Z} : a^m = e\}$ は $\boldsymbol{Z}$ の部分群であり，したがって，ある正数 n_a に対して $< n_a >$ と一致する (例 2 ）. 準同型定理 (後述）によれば，商群 $\boldsymbol{Z}/ < n_a >$ は，$< a >$ と同型である．

G の元 a に対して, 自然数 n があって $a^n = e$ が成り立つとき，a は**位数有限**であるという．またこのとき，このような n の最小のものを a の**位数** という．

例 4　C^* は有限群を含んでいる．複素数 $\omega = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$ に対して,

$$\{1, \omega, \omega^2, ..., \omega^{n-1}\}$$

は位数 n の有限巡回群である．（C^* の有限部分群は巡回群である.）

例 5　位数 n の群は，S_n の部分群として実現できる．

例 6　n 次の偶置換全部の集合 A_n は，対称群 S_n の部分群である．そのほか，たとえば，4 次の置換

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

は S_4 の部分群をつくる．

例 6　$SL(n, \boldsymbol{R})$ は $GL(n, \boldsymbol{R})$ の正規部分群である．

1.5.3 同値類と商群

H を G の部分群とする．G の元 x, y が

$$x^{-1}y \in H$$

を満たすとき，$x \sim y$ と書く．この関係は同値関係

$$(1)x \sim x \quad (2)x \sim y \Rightarrow y \sim x \quad (3)x \sim y, y \sim z \Rightarrow x \sim z$$

をみたすので，x と y は同値であるという．

各 x に対して， x を含む同値類はただ一つである．それは，xH である．x を同値類 xH の代表元という．この同値類をを**左同値類**という．各同値類から代表元を 1 つずつ選んでそれらの集合 T を左代表系という．

$$G = \sum_{t \in T} tH$$

と書くことができる．同じように右同値類が定義され，Hx の形に書ける．右同値類を T' とすれば

$$G = \sum_{t \in T'} Ht$$

と書ける．次のことが成り立つ：
(1) T が左代表系ならば T^{-1} は右代表系である．
(2) 左同値類の集合 G/H と，右同値類の集合 $G\backslash H$ は 1 対 1 に対応する．

とくに，H が G の正規部分群であるときは，すべての x に対して，左同値類 xH と右同値類 Hx は一致する．またこのとき，同値関係と演算が両立する：

$$a \sim a', \quad b \sim b' \quad \Rightarrow \quad ab \sim a'b'$$

したがって同値類の集合は群となる．これを**商群 facter group** といい，G/H で表す．G/H の位数を G における H の指数といい，$[G : H]$ で表す..

1.5.4 準同型

群 G から群 G' への写像 f が

$$f(ab) = f(a)f(b), \quad ab \in G$$

を満たすとき, f を G から G' への**準同型写像 homomorphism** という．このとき

$$Kerf = \{x \in G : f(x) = e'\}$$

$$Imf = \{x' \in G' : x' = f(x),\ \ x \in G\}$$

とおく．$Kerf$ を f の**核 kernel**，Imf を f の**像 image** という．

f が G から G' へ準同型写像であるとき，定義から次のことがわかる．
(1)　G と G' の単位元をそれぞれ e, e' とするとき $f(e) = e'$
(2)　$f(x)^{-1} = f(x^{-1})$
(3)　$Kerf$ は G の正規部分群である．
(4)　Imf は G' の部分群である．
(5)　f が単写であるための必要十分条件は $Kerf = \{e\}$ である

準同型写像 f が全単写であるとき，f を**同型写像 isomorphism** という．G から G' への同型写像があるとき，G と G' は**同型**であるといい，$G \cong G'$ とかく．

G から G 自身への同型写像を**自己同型写像 automorphism** という．G の元 a に対して, 写像

$$x \mapsto x^* = axa^{-1}$$

は G の自己同型写像である．これを (a によって引き起こされる） G の**内部自己同型写像**という．このとき，x^* を x の**共役元**という．内部自己同型写像以外の自己同型写像を**外部自己同型写像**という．
内部自己同型写像によって，G の部分群 H は部分群 $H_a^* = aHa^{-1}$ に写される．H_a^* を H の**共役部分群**という．すべての a に対して，$H_a^* = H$ が成り立つとき，　H は G の正規部分群である．

定理 1.5.1 (準同型定理)　f が G から G' の上への準同型写像であるとき,

$$N = Kerf$$

による商群 G/N は G' と同型である．また逆に, G の正規部分群 N が与えられたとき，写像

$$x \mapsto xN$$

は，G から G/N の上への準同型写像である．(これを**自然な準同型写像 natural homomorphism** という.)

(証明) G の元 x, y に対して
　x と y が同値　$\Leftrightarrow$　$x^{-1}y \in N$
$\Longleftrightarrow$　$f(x^{-1}y) = e' \Longleftrightarrow$　$f(x^{-1})f(y) = e'$
　$\Longleftrightarrow$　$f(x)^{-1}f(y) = e' \Longleftrightarrow$　$f(x) = f(y)$

が成り立つ．したがって

$$\varphi : xN \mapsto f(x)$$

によって G/N から G' への写像 φ が定義され，1 対 1 準同型である．□

1.5.5 同型定理

定理 1.5.2 (第１同型定理) f は G から G' の上への準同型写像であるとする．H' が G' の正規部分群であるとき，$H = f^{-1}(H')$ は G の正規部分群で

$$G/H \cong G'/H'$$

(証明) G' の H' による同べつで，$a' \in G'$ を含む同値類を $[a']$ で表すことにする．写像 $f^* : G \to G'/H'$ を

$$f^*(x) = [f(x)], \qquad x \in G$$

で定義すると，f^* は G から G'/H' の上への準同型写像である．H' は G'/H' の単位元であるから，$H = f^{-1}(H') = Kerf^*$. したがって H は G の正規部分群で，準同型定理により $G/H \cong G'/H'$. □

系 H と N が G の正規部分群で，$N \subset H$ であるとき

$$(G/N)/(H/N) \cong G/H$$

定理 1.5.3 (第２同型定理) H は G の部分群, N は G の 正規部分群ならば $H \cap N$ は H の 正規部分群で

$$HN/N \cong H/H \cap N$$

1.6 環

集合 R が**環 ring** であるとは加法と乗法が定義され，次の条件を満たすことであった．(x, y, z は R の元)．

(1) R は加法群である：

(2) 乗法は

$$x(yz) = (xy)z \qquad \text{を満たす.}$$

(3)　R は乗法の単位元 1 をもつ.
(4)　分配則 $x(y+z)=xy+xz,\quad (x+y)z=xz+yz$ を満たす.

（注）条件 (3) を省略する定義もある.

環 R の元 $a\neq 0$ に対して，元 $b\neq 0$ があって，$ab=0$ または $ba=0$ が成り立つとき，a を**零因子 zero diviser** という．0 でない元をもち，かつ 0 以外に零因子をもたない環を**整域 integral domain** という.

例 1 整数全部の集合 $\boldsymbol{Z}$ は整域である.
例 2 多項式全部の集合は整域である.
例 3 ある区間で連続な関数全部の集合は環である．整域ではない
例 4 $\boldsymbol{Z}_m$ は環である．m が素数でないときは整域ではない．m が素数のときは整域である（体になる）.
例 5 平面領域 D で正則な関数全部の集合は整域である．D で連続な関数全部の集合は整域ではない.
例 6 $n\times n$ 実行列全部の集合 $M(n,\boldsymbol{R})$ は非可換環である.

環 R から環 R' への写像 f が次の条件を満たすとき，準同型写像という.
(1)　$f(x+y)=f(x)+f(y)$
(2)　$f(xy)=f(x)f(y)$
(3)　$f(1)=1'$　　（$1'$ は R' の単位元）
準同型対応 f について $\mathrm{Ker}f=f^{-1}(\{0\})$ を f の**核 kernel** という.

定理 1.6.1 (準同型定理)

$$R/\mathrm{Ker}f\cong \mathrm{Im}f$$

文字 x の形式的な式

$$f(x)=a_nx^n+\cdots+a_1x+a_0\quad a_i\in R$$

を R 上の多項式という．$a_n\neq$ のとき，n を f の**次数 degree** といい，$\deg f$ と書く．R 上の多項式全部の集合は，形式的な和および積によって環になる．これを R 上の**多項式環 polynomial ring** といい，$R[x]$ で表す.
R が可換であれば $R[x]$ も可換である．R が整域であれば $R[x]$ も整域である.

定理 1.6.2 R は可換環，$f, h \in R$ で，h の最高次の係数は可逆元であるとする．このとき $q, r \in R[x]$ が存在して

$$f = qh + r, \qquad \deg r < \deg h$$

多項式 $f(x)$ に対して，$f(a) = 0$ を満たす $a \in R$ を $f(x)$ の**根 root** という．

定理 1.6.3 (因数定理) $\boldsymbol{a} \in R$ が $f(x)$ の根であるための必要十分条件は

$$f(x) = (x - a)g(x) \qquad g \in R[x]$$

が成り立つことである．

環 R の部分集合 I が次の条件を満たすとき**イデアル ideal** という．

(1) I は加法群である．

(2) 任意の $a \in I$ と任意の $x \in R$ に対して $ax \in I$, $xa \in I$.

I と J がイデアルであるとき,

$$I + J = \{a + b : a \in I, b \in J\}, \quad IJ = \{ab : a \in I, b \in J\}$$

もイデアルである．

$a_1, \ldots, a_m \in R$ に対して，集合 $\{\lambda_1 a_1 + \cdots + \lambda_m a_m : \lambda_i \in R\}$ は R のイデアルになる．これを $a_, \ldots, a_m$ によって生成されるイデアルという．1 つの元 a によって生成されるイデアルを**単項イデアル principal ideal** という．

$1 \in I$ ならば $I = R$ となる．

$a, b \in R$ について，$a - b \in I$ が成り立つとき $a \sim b$ と定義すると，商集合 $R/\sim$ は環となる（剰余環）．これを R/I で表す．

イデアル $I \quad (I \neq R)$ が

$$ab \in I \Longrightarrow a \in I \text{ または } b \in I$$

を満たすとき, すなわち R/I が整域であるとき，I を**素イデアル prime ideal** という．

イデアル $I \quad (I \neq R)$ が

$$I \subset J \text{ となるイデアル } J \text{ があれば } J = I \text{ または } J = R$$

を満たすとき，すなわち R/I が体であるとき，I を**極大イデアル maximal ideal** という．極大イデアル は素イデアルである．

1.7　（可換）体

K が可換環で，$0 \neq 1$ で，0 以外の元が可逆であるとき，K は**体 field** であるという．乗法の可換性を仮定しないときは**斜体 skew field** という．（有限な斜体は可換であることが知られている．）

例 1　$\boldsymbol{R}$, $\boldsymbol{Q}$, $\boldsymbol{C}$ は体である．

例 2　R 上の 2 次元ベクトル空間 で，その基底を $1, i$ とするとき，乗法の規則

$$11 = 1, ii = -1, 1i = i1 = i$$

を与えることにより，この空間は可換環をつくる．ai を a と同一視して，その元を

$$a + bi$$

と書くことにする．$a^2 + b^2 \neq 0$ のとき，$a + bi$ の逆要素を $(a^2 + b^2)^{-1}(a - bi)$ と定義することにより，（可換）体ができる．これが複素数体 $\boldsymbol{C}$ である．

例 3　R が整域であるとき，$R^* = R \setminus \{0\}$ と書くことにする．$R \times R^*$ において，$(a, b) \sim (a', b')$ であるとは $ab' - a'b = 0$ であると定義し，(a, b) を含む同値類を a/b で表す．算法

$$a/b + c/d = (ad + bc)/bd, \qquad a/b \cdot c/d = ac/bd$$

によって商集合 $(R \times R^*)/\sim$ は体となる．これを R の **商体 quotienr field** といい，$Q(R)$ で表す．$Q(\boldsymbol{Z}) = \boldsymbol{Q}$ である．（微分方程式の形式的解法を正当化したミクシンスキーの演算子法はこの考えを利用したものである．）

例 4　体 K は $\boldsymbol{R}$ または $\boldsymbol{Q}$ とする．$\boldsymbol{H}$ は K 上の 4 次元ベクトル空間とし，その基底 e, j, k, l の間に乗法の規約

$$ee = e, \quad jj = kk = ll = -e, \quad ej = Je = j, \quad ek = ke = k, \quad eL = Le = l$$

$$jk = l, kj = -l, \quad kl = j, \quad lk = -j, \quad lj = k, \quad jl = -k$$

が与えられてるとする．これによって，$\boldsymbol{H}$ は非可換な環となる．ae を a と同一視して，

$$a + bj + ck + dl, \ a, b, c, d, \in K$$

を**四元数 Quaternion** という．$a^2 + b^2 + c^2 + d^2 \neq 0$ のとき，$a + bj + ck + dl$ の逆元を

$$\frac{1}{a^2 + b^2 + c^2 + d^2}(a + bj + ck + dl) = a - bi - cj - kl)$$

と置くことにより，$\boldsymbol{H}$ は斜体となる．これを**四元数体**という．$\boldsymbol{R}$ を係数体とする有限次元の多元体は，$\boldsymbol{R}$, $\boldsymbol{C}$, $\boldsymbol{H}$ に限る．

例 5　p が素数のとき，剰余環 $\boldsymbol{Z}_p$ は体である．

例 6　有限な整域は体である

体のいくつかの部分体の共通部分は体である．
体の部分環は整域である．体の有限部分環は体である．

体 K の任意の部分集合 S に対して，S を含む部分体の共通部分をその体の上で S が生成する体という．

体 K の部分体が K 以外にないとき，K を **素体**という．1 が生成する K の部分体 P は素体である．P が有限体であるとき，P の元の個数 p を K の**標数 chracteristic** という．P が無限であるときは K の標数は 0 であると定義する．たとえば，実数体 $\boldsymbol{R}$ や複素数体 $\boldsymbol{C}$ は標数 0 である．
標数 0 のときは，P は有理数体 Q と同型である．標数 p が 0 でないときは，P は $\boldsymbol{Z}_p$ と同型で p は素数である．またこのとき，写像

$$x \mapsto x^p$$

は K から K への同型写像であり

$$(x+y)^p = x^p + y^p, \qquad (x-y)^p = x^p - y^p \qquad (x, y \in K)$$

が成り立つ．とくに，K が有限体のときは，上の写像は K の置換であり，K の自己同型写像である．

有限体の標数は勿論素数である．有限体 K の標数を p とすると，$|K|$ は p のべき p^n となる．また逆に，任意の自然数 n と任意の素数 p に対して $|K| = p^n$ となる体 K が存在する．

K_1 が体 K の部分体であるとき，K を K_1 の拡大体であるという．ある体の部分体 K と部分集合 T に対して，$T \cup K$ で生成される部分体を, K に T を付加した体といい，$K(T)$ と書く．T が有限集合のときには $K(T)$ は K 上有限生成の体であるという．とくに，1 つの元 x を付加した体 $K(x)$ を単純拡大という．

K の拡大体 L は K 上の線形空間と考えることができる．この線形空間の次元を拡大 $K \subset L$ の**（拡大）次数**とよび $[L : K]$ で表す．次数有限の拡大を**有限拡大**という．L の元 α に対して，0 でない多項式 $f(x) \in K[x]$ があって $f(\alpha) = 0$ となるとき α は K 上**代数的 algebraic** であるという．代数的でない元は**超越的 transcendental** であるという．

演 習　1

1. 複素数体は順序体でないことを証明せよ.

2. (1) $e^{i(\theta_1+\theta_2)} = e^{i\theta_1}e^{i\theta_2}$ を示せ.
   (2) 数学的帰納法を用いて，de Moivre の公式を証明せよ.

3. $a^{n+1} - (a+1)^{2n+1}$ は $a(a+1)+1$ で割り切れることを示せ.（n は自然数：たとえば $3^{n+1} + 4^{2n-1}$ は 13 で割りきれる.：数学的帰納法）

4. $C(\boldsymbol{R})$ 上の内積空間 V において，次の等式を示せ.
   (1) $\| \boldsymbol{a} + \boldsymbol{b} \| = \| \boldsymbol{a} \|^2 + 2\mathrm{Re}\langle \boldsymbol{b}, \boldsymbol{a} \rangle + \| \boldsymbol{b} \|^2$
   (2) $|\langle \boldsymbol{a}, \boldsymbol{b} \rangle| \leqq \| \boldsymbol{a} \| \| \boldsymbol{b} \|$
   (3) $\| \boldsymbol{a} + \boldsymbol{b} \| \leqq \| \boldsymbol{a} \| + \| \boldsymbol{b} \|$

5. 群の条件 (G_2), (G_3) は次の条件に置き換えることが出来ることを示せ.
   $(G_2)' \exists e \in G; ea = a \quad \forall a \in G$
   $(G_3)' \forall a \in G, \exists a'; a'a = e$

6. 群において，単位元および逆元はただ 1 つであることを示せ.

7. 環 R において，任意の元について次の式を示せ.

$$0\ a = a\ 0 = 0$$

8. T が左代表系であれば，T^{-1} は右代表形であるとを示せ.

9. H が G の部分群で, K が H の部分群ならば
   (1) $[G : K] = [G : H][H : K]$
   (2) T, T' がそれぞれ H, K の代表系ならば，TT' は K の代表系である.

10. 群 G の位数が素数 p であるとき，G は巡回群であることを示せ.

11. 加法群 $\boldsymbol{Z}$ の部分群 H は，ある $n \in \boldsymbol{Z}$ によって生成される巡回群 $< n >$ であることを示せ.

12. 位数４の群 G は，次の２種類であることを示せ.
    (1) G は位数４の巡回群である.
    (2) G の単位元以外の要素の位数は，すべて２で，G は可換である.
    （(2) の場合の群 G を，クラインの４元群という.）

13. 群 G の有限部分集合 H について

$$a, b \in H \Longrightarrow ab \in H$$

が成り立つならば，H は G の部分群であることを証明せよ. とくに，$G = C^*$ のときは, H は

$$H = \{1, \exp\left(i\frac{2\pi}{n}\right), \ldots, \exp\left(i\frac{2(n-1)\pi}{n}\right)$$

の形であることを示せ.

14. 指数２の部分群は正規部分群であることを示せ.

15. 群 G の部分群

$$Z = \{x \in G : \forall a \in G, ax = xa\}$$

を G の**中心**という. 中心はアーベル群で, G の正規部分群である.

16. 群 G の部分群 H に対して

$$N(H) = \{x \in G : Hx = xH\}$$

を H の**正規化群**という. H は $N(H)$ の正規部分群である. $N(H)$ は H を正規部分群として含む最大の部分群である. とくに, $N(H) = G$ ならば，H は G の正規部分群である.

17. 群 G の元 a, b に対して， $a^{-1}b^{-1}ab$ を G の交換子という.
    G のすべての交換子から生成される部分群 K を G の**交換子群**という.
    H が G の正規部分群でかつ G/H がアーベル群であるための必要十分条件は，$K \subset H$ である. とくに，交換子群 K は正規部分群である.

18. 群 G の元 a に対して，$t^{-1}at = b$ の形の元 b を a の**共役元**という. 部分群 H の任意の元の共役元が H に属するとき, H は G の正規部分群である.

19. 部分群 H に対して，$t^{-1}Ht = H'$ $t \in G$ の形の部分群 H' を H の**共役部分群**という．部分群 H の共役部分群全部の共通集合は正規部分群である．

20. 準同型写像の性質 (1) - (5) (p.31) を示せ．

21. 部分群のどちらかが正規部分群であれば，HH' は部分群である．
H, H' がともに正規部分群であれば，HH' は正規部分群である．

22. n 次の置換は，巡回置換の積で表される．

23. 対称群 S_n は，２つの置換 $\sigma = (1, 2), \quad \tau = (1, 2, ..., n)$ で生成される．

24. 偶置換は ３次の巡回置換の積で表される．

25. G は集合 Ω の置換群であるとする．$\omega \in \Omega$ に対して, $g(\omega) = \omega$ を満たす g 全部の集合は G の部分群である

26. G は集合 Ω の置換群であるとする．置換 g によって不変な Ω の要素の個数を $\psi(g)$ で，また Ω の要素 x に対して，x を不変にするような G の要素の個数を $\eta(x)$ で表すと
$$\sum_{x \in \Omega} \eta(x) = \sum_{g \in G} \psi(g)$$

27. 四元数 $q = a + bi + cj + dk$ において，$v = (a, b, c)$ として $q = (a, V)$ と表すことにし，$(a, \mathbf{0})$ は実数 a と同一視する．演算は
$$q_1 + q_2 = (a_1 + a_2, V_1 + V_2), \quad \lambda q = (\lambda a, \lambda V) \qquad (\lambda \in \boldsymbol{R})$$
$$q_1 q_2 = (a_1 a_2 - V_1 \cdot V_2, \ \ a_1 V_1 + a_2 V_2 + V_1 \times V_2)$$
と書けることを示せ．

第2章　組合せ理論

2.1　順列と組合せ

2.1.1　順列

n 個の相異なるものから m のものを選んで，順番をつけて並べることを**順列 permutaion** という．この順列の総数を ${}_nP_m$ と書くことにすると

$$ {}_nP_m = n(n-1)(n-2)\cdots(n-m+1) = \frac{n!}{(n-m)!} \tag{2.1} $$

である．とくに, $n = m$ のときには, ${}_nP_n = n!$ であるが, これは, 番号のついた n 個のものの並べ替えの総数である．これを n 次の置換ともいう．

なお, $0! = 1$ と約束しておくと便利である．

n 個の相異なるものから m 個のものを選び出すときに, 同じものを何回も選んでもよいことにしたものが**重複順列 repeated permutaion** である．その総数は，n^m に等しい．

例 1.1　n 人の人がまるく輪になって並ぶ方法は何通りあるか．　(円順列)
(解 1）n 人の人が 1 列に並ぶ方法は $n!$ 通りある．これを輪にすると, 輪を回転しても変わらないから, 回転の仕方 n で割って $n!/n = n-1!$ 通りある．
(解 2）特定の 1 人の位置の決め方は自由であるから, それを固定しておいて他の $n-1$ 人の並べ方は $(n-1)!$ 通りである．

つぎに, k 種類のものからなる n 個のものがあり, 第 1 の種類は m_1 個, 第 2 の種類は m_2 個, .., 第 k の種類は m_k 個あるとする．同じ種類のものは区別しないものとすれば, 並べ方の総数は

$$ \frac{n!}{m_1!m_2!\cdots m_k!} \tag{2.2} $$

である．

例 1.2　$720!$ は $(6!)^{120}$ で割りきれることを示せ．
一般に, $(n!)!$ は $(n!)^{(n-1)!}$ で割りきれる．
(解）6 個ずつ $5!$ 種類のものがあるとすると、総数は $6 \cdot 5! = 6! = 720$ である．これを並べる方法は $\dfrac{720!}{(6!)^{5!}}$ 通りあるが, この数は整数である．

例 1.3　長点 ー と短点 ・ を５個まで使って何通りの信号が作れるか.　また, 長点は３個までしか使えないことにすると何個あるか,
(解)　まず, ５個使う場合を考える. 長点を５個使う方法は１通り, 長点を４個と短点を１個並べる方法は $\frac{5!}{4!1!} = 5$ 通り, 長点３個と短点２個を並べる方法は $\frac{5!}{3!2!} = 10$ 通り, 長点２個と短点３個を並べる方法も１０通り, 長点１個と短点４個を並べる方法は５通り、短点５個を並べるのは１通り合計３２通りある. 同様に４個の場合は $1+4+6+4+1=16$ 通り, ３個の場合は $1+3+3+1=8$ 通り, ２個の場合は $1+2+1=4$ 通り, １個の場合は $1+1=2$ 通りある. これらを合計して,　62 通りある.

もう１つの考え方は,　５個の場合, ２つのものから５個を選ぶ重複順列であるから, 2^5 通り, ４個の場合は 2^4 個, ３個の場合は 2^3 個, ２個の場合は 2^2 個, １個の場合は 2^1 個あるから, 総計は

$$2^5 + 2^4 + 2^3 + 2^2 + 2^1 = \frac{2^6 - 2}{2 - 1} = 62 \text{ 通り}.$$

長点が３個までしか使えない場合には,

$$(10+10+5+1+1)+(4++6+4+1)+(1+3+3+1)+(1+2+1)+(1+1) = 55 \text{ 通り}$$

なお, ${}_nP_m$ を n の多項式 $P(n)$ と考えて,　n を x と書きなして

$$\begin{aligned} P(x) &= x(x-1)(x-2)\cdots(x-m+1) \\ &= s(m,m)x^m + s(m,m-1)x^{m-1} + \cdots + s(m,0) \end{aligned}$$

としたとき, x^k の係数 $s(m,k)$ を**第 1 種スターリング数 (Stirling number)** という. $k > m$ のときは $s(m,k) = 0$ と約束する.

$$s(m+1,k) = s(m,k-1) - ms(m,k)$$

$$s(m,m) = 1, \qquad m \geq 1$$

$$s(0,0) = 0$$

が成り立つ.

2.1.2　組合せ

n 個の相異なるものから m のものを選びだすことを**組合せ combination** という. その総数は

$$\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{m!} = \frac{n!}{m!(n-m)!} \tag{2.3}$$

である. $\binom{n}{m}$ の代わりに, ${}_nC_m$ または $C(n,m)$ とも書く.
(1.3) の右辺は, n が任意の実数であるときにも意味をもつ. そこで, 任意の実数 α に対して

$$\binom{\alpha}{m} = \frac{\alpha(\alpha-1)\cdots(\alpha-m+1)}{m!} \tag{2.4}$$

と定義する.

例 1.4 1 から 300 までの数のうちから 3 つの数を選んで, その和が 3 で割りきれるようにしたい. 幾通りの選び方があるか.
(解) 3 で割り切れる数の集合を A, 3 で割って 1 余る数の集合を B, 3 で割って 2 余る数の集合を C とする. 3 つの集合に含まれる数の個数は 100 ずつである. 選び方は, どれか 1 つの集合から 3 つ選ぶか, または 3 つの集合から 1 つずつ選ぶかである. その総数は

$$\binom{100}{3} + \binom{100}{3} + \binom{100}{3} + (100)^3 = 1,485,100 \text{ 通り}$$

2.1.3 2 項係数

$\binom{n}{m}$ を **2 項係数 binomial coefficient** というが, それは **2 項定理 binomial theorem**：

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{m}a^{n-m}b^m + \cdots b^n \tag{2.5}$$

の右辺の係数だからである..
2 項係数の性質：
(1) $\binom{n}{m} = \binom{n}{n-m}$
(2) $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$
(3) $\sum_{k=0}^{n}(-1)^k \binom{n}{k} = 0$
(4) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
(5) $\sum_{k=0}^{n} \binom{n}{k} x^k(1-x)^{n-k} = 1$
(6) $\sum_{k=0}^{n} k \binom{n}{k} = n2^{n-1}$
(7) $\sum_{k=0}^{n} k \binom{n}{k} x^k(1-x)^{n-k} = nx$

(8) $\displaystyle\sum_{k=0}^{n} k(k-1)\binom{n}{k}x^k(1-x)^{n-k} = n(n-1)x^2$

(9) $\displaystyle\sum_{k=0}^{n}(k-np)^2\binom{n}{k}p^k(1-p)^{n-k} = np(1-p) \quad (0 \leqq p \leqq 1)$

(10) $\displaystyle\sum_{k=0}^{m}\binom{n}{k}\binom{l}{m-k} = \binom{n+l}{m}$

(11) $\displaystyle\binom{n}{k}^2 \geqq \binom{n}{k-1}\binom{n}{k+1}$

ここまでは n は自然数であるが，負の整数の場合も後で用いる．このときは

$$\binom{-m}{r} = (-1)^r\binom{m+r-1}{r}$$

が成り立つ．

2.1.4 写像による表現

与えられた n 個のものに番号をつけておくと，これらのものの集合は，集合 $R = \{1, 2, .., n\}$ と同等である．n 個のものから m 個のものを選び出す順列は，m 個の番号 $1, 2, ..m$ を R のうちの m 個のものに割り当てることであるから，集合 $D = \{1, 2, ..m\}$ から R の中への単写である．

とくに，n 個のものの順列は，全単射 $f : D \to D$ である．

重複順列は, 順列の場合の単射という条件を取り除いたもので，その総数は，D から R への写像全部の個数 n^m に等しい.

n 個のものから m 個のものを選び出す組み合せは，D から R への写像 f において，その値はどの順序に並べても同じであると見るのであるから，数 $f(i)$ を小さい方から順に並べることにすると

$$f(i) < f(i+1), \quad i = 1, ..m-1$$

を満たす写像 (単射） $f : D \to R$ である．

2.1.5 重複組合せ

n 個の相異なるものから m のものを選びだすときに，同じものを何回も選んでもよいことにしたものが，**重複組合せ repeated combination** である．重複を許すということは，組合せを表現する関数 f が

$$f(i) \leqq f(i+1), \quad i = 1, .., m-1$$

を満たすということである．そこで

$$g(i) = f(i) + i - 1, \quad i = 1, .., m$$

によって，新しい写像 g を定義すれば，g は D から集合 $\{1, 2, .., n+m-1\}$ への単写で，$g(i) < g(i+1)$ を満たしている．したがって，重複組合せの総数は，$n+m-1$ 個のものから m 個選ぶ組合せの総数

$$\binom{n+m-1}{m} \tag{2.6}$$

に等しい.

2.1.6　分配の問題

異なるものを異なる部屋に分配する問題

k 個の異なるものを n 個の異なる部屋へ分配することは, n 個のものから k 個のものを重複を許して選び出す順列である．　それはまた, 集合 $D = \{1, 2, \ldots k\}$ から 集合 $R = \{1, 2, \ldots n\}$ への写像である. その総数は n^k である。もし, どの部屋にも少なくとも１つは入れる $(n \geqq k)$ ことにするなら, それは R から D への全射である.

同種のものを異なる部屋へ分配する問題

k 個の同種のものを n 個の異なる部屋へ分配するのに次の３つの場合の総数を求める.

(1) どの部屋にも２つ以上は入らない場合

(2) どの部屋にもいくつでも入る場合

(3) どの部屋にも m 個以上いれる場合（この場合は $k - mn \geqq 0$)

(1) は，k 個のものを置く部屋を n 個の部屋から選び出す仕方の総数であるから，$\binom{n}{k}$ に等しい.

(2) は，k 個のものと，区別のない $n-1$ 個の間仕切りの順列であるから $\binom{n-1+k}{k}$ に等しい．これは n 個のものから重複を許して k 個選び出す仕方の総数に等しく，またこれは

$$x_1 + \cdots + x_n = k$$

の負でない整数解の総数に等しい.

(3) は，各部屋にあらかじめ m 個のものを入れておき，そのあとで残りの $k - mn$ 個のものを分配する仕方であるから，総数は $\binom{n+k-mn-1}{k-mn}$ に等しい.

例 1.5　異なる５個の文字を送信するのに，合計１５個の空白を文字の間に挿入したい. いく通りの列ができるか．どの場所にも３個以上挿入のときはどうか.

(解)　１通りの文字の並べ方について １５個の空白を４つの字間に挿入する仕方は $\binom{15+4-1}{15}$ 通り であるから 5! 倍して 97,920 通り．　３個以上挿入のときは $5! \times \binom{15-12+4-1}{15-12} =$ 2400 通り に等しい.

異なるものを同種の部屋に分配する問題

n 個の相異なるものを同種の k 個の部屋に, どの部屋にも少なくとも１つは入るように分配することは n 個の相異なるものを k 個のグループに分割することである．その総数を $S(n, k)$ で表し, これを**第２種スターリング数**という．この場合, $k \leqq n$ であるが, $k > n$ については $S(n, k) = 0$ と約束する.

$$S(n, k+1) = S(n, k-1) + kS(n, k), \qquad (n \geq k \geq 1) \tag{2.7}$$

$$S(n,1) = S(n,n) = 1 \qquad (n \geq 1) \tag{2.8}$$

が成り立つ. $S(n,k)$ の値の計算は, 後の節で述べる. n 個の相異なるものを k 個の相異なる部屋に, 分配する仕方の総数は $k!S(n,k)$ に等しい. いま $n \leq m$ として, 集合 $D = \{1,2,\dots n\}$ から 集合 $R = \{1,2,\dots m\}$ への写像を考えると, その総数は m^n である. この写像を値の個数によって分類する. 値の個数は n より大きくならない. $k \leq n$ として, k 個の元を持つ R の任意の部分集合 I に対して, I を値の集合にもつ写像は D から I への全射であるからその総数は. $k!S(n,k)$ に等しい. R から k 個の元を持つ部分集合を選び出す方法は $\binom{m}{k}$ 通りあるから, 値の個数が k であるような写像の総数は $\binom{m}{k}k!S(n,k)$ に等しい. D から R への写像の総数は, 値の個数が k であるような写像の総数を k について 1 から n まで加えたものである. これが m^n に等しいから

$$m^n = \sum_{k=0}^{n} \binom{m}{k} k!S(n,k) = \sum_{k=0}^{n} S(n,k)m(m-1)\cdots(m-k+1) \tag{2.9}$$

が成り立つ. このことは任意の $m \quad (m \geq n)$ 対して成立する. そこで, x の多項式

$$f(x) = x^n, \qquad g(x) = \sum_{k=0}^{n} S(n,k)x(x-1)(x-k+1) \tag{2.10}$$

を考えると, 任意の $m \quad (m \geq n)$ 対し $f(m) = g(m)$ が成り立つことになり, したがってすべての x に対して $f(x) = g(x)$ が成り立つ. すなわち

$$x^n = \sum_{k=0}^{n} S(n,k)x(x-1)\cdots(x-k+1) = \sum_{k=0}^{n} \binom{x}{k} k!S(n,k) \tag{2.11}$$

が成り立つ.

n 個の相異なるものを空でないグループに分割する仕方の総数は, 各 k について計算した数の和 $\sum_{k=1}^{n} S(n,k)$ である. これを**ベル数**といい, B_n で表す.

2.2 反転公式

数学には**反転公式 inversion formula** と呼ばれるものがたくさんある. たとえばフーリエ変換やラプラス変換の反転公式などがある. 要するに, ある変換に対してその逆変換を与える公式である. その最も初等的なものは, 正則行列による変換の逆変換, つまり逆行列によってあたえられるもおで, ここで述べる公式は, それの応用である.

2.2.1 反転公式の原理

$n = 0, \cdots, N$ に対して, $p_n(x), q_n(x)$ は, n 次の多項式で, 最高次の係数が 1 であるとする.

いま, 等式

$$\sum_{k=0}^{N} a_{ik} p_k(x) = q_i(x) \qquad i = 0, \cdots, N \tag{2.12}$$

$$\sum_{k=0}^{N} b_{jk} q_k(x) = p_j(x) \qquad j = 0, \cdots, N \tag{2.13}$$

が成り立っているならば, $x_0, \cdots, x_N$ と $y_0, \cdots, y_N$ に対して

$$\sum_{k=0}^{N} a_{ik} x_k = y_i \qquad i = 0, \cdots, N \tag{2.14}$$

が成り立つことと

$$\sum_{k=0}^{N} b_{jk} y_k = x_j \qquad j = 1, \cdots, N \tag{2.15}$$

が成り立つことは同値である. これが反転公式の原理である.

N 次以下の多項式全部の集合 V は $N+1$ 次元の線形空間をつくる. $\{p_n(x)\}, \{q_n(x)\}$ は, それぞれ, V の基底である. したがって, 等式 (1) が成り立つということは, 行列 $B = (b_{ij})$ が $A = (a_{ij})$ の逆行列であることを示している. これが反転原理の成り立つ理由である.

もし，A が三角行列である場合，すなわち，$k > n$ に対して，$a_{nk} = 0 \quad b_{nk} = 0$ が成り立つ場合には，上の式は

$$\sum_{k=0}^{n} a_{nk} p_k(x) = q_n(x), \quad \sum_{k=0}^{n} b_{nk} q_k(x) = p_n(x)$$

$$\sum_{k=0}^{n} a_{nk} x_k = y_n, \quad \sum_{k=0}^{n} b_{nk} y_k = x_n$$

となっていることに注意する．２項係数や，第１種，第２種のスターリング数はこの条件を満たしている.

2.2.2　２項係数の反転公式

２項定理によって, 任意の n に対して

$$x^n = (x - 1 + 1)^n = \sum_{k=0}^{n} \binom{n}{k} (x-1)^k \tag{2.16}$$

および

$$(x-1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} x^k \tag{2.17}$$

が成り立つ. x^n と $(x-1)^n$ は n 次の多項式で, x^n の係数が 1 であるからから, $x_1, \cdots, x_m$ と $y_1, \cdots, y_m$ に対して

$$x_n = \sum_{k=0}^{n} \binom{n}{k} y_k \qquad n = 1, \cdots, m \tag{2.18}$$

が成り立つことと

$$y_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} x_k \qquad n = 1, \cdots, m \tag{2.19}$$

が成り立つことは同値である.

2.1.6 で述べたように

$$n^m = \sum_{k=0}^{n} \binom{n}{k} k! S(m,k) \tag{2.20}$$

が成り立つ. これに反転公式を適用すると

$$S(m,n) = \frac{1}{n!} \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^m \tag{2.21}$$

が得られる. これは, 後述の (2.33) と同じである.

2.2.3 スターリング数の反転公式

第 1 種スターリング数 $s(n,k)$ と第 2 種スターリング数 $S(n,k)$ についてはそれぞれ次の公式がある：

$$x(x-1)\cdots(x-n+1) = \sum_{k=1}^{n} s(n,k) x^k \quad n = 1, \cdots, m \tag{2.22}$$

$$x^n = \sum_{k=1}^{n} S(n,k) x(x-1)\cdots(x-k-1) n = 1, \cdots, m \tag{2.23}$$

x^n と $x(x-1)\cdots(x-n+1)$ はどちらも n 次の多項式で x^n の係数は 1 である. したがって, $x_1, \cdots, x_m$ と $y_1, \cdots, y_m$ に対して

$$\sum_{k=1}^{n} s(n,k) x_k = y_i \qquad i = 1, \cdots, m \tag{2.24}$$

が成り立つことと

$$\sum_{k=1}^{n} S(n,k) y_k = x_j \qquad j = 1, \cdots, m \tag{2.25}$$

が成り立つことは同値である.

2.3　母関数

2.3.1　通常母関数

いくつかの異なるもの $\{a, b, c, ...\}$ のうちから a を選ぶことを記号で a で表す. a か b を選ぶということを記号で　$a+b$ で表し，a と b の両方を選ぶということを記号で ab で表す. また，どちらも選ばないことを 記号 1 表す.
３つ以上の場合も同様である.　異なる３つのもの a, b, c からどれか１つを選ぶ選び方は

$$a+b+c$$

で，これらのうちからどれか２つを選ぶ選び方は

$$ab+bc+ca$$

で，３つ全部を選ぶ選び方は

$$abc$$

で表す。どれも選ばないことを１で表す. a についても b についても c についても選ぶか選ばないかの選択があるとすれば, a, b, c についての選び方は

$$(1+a)(1+b)(1+c) = 1+(a+b+c)+(ab+bc+ca)+abc \tag{2.26}$$

の式で表される. もし, a, b, c の間に区別をつけず, 選び方の数だけに興味がある場合には, $a=b=c=x$ とおくと (2.26) は次の式になる：

$$(1+x)^3 = 1+3x+3x^2+x^3 \tag{2.27}$$

右辺の式は, 選ばない仕方１通り, １個選ぶ方法は３通り, ２個選ぶ方法は３通り, ３個選ぶ方法は１通りということを表していて, x^k の係数は, ３個のうちのどれか k 個を選ぶ選び方を表している．x^0 の係数は 1 で，なにも選ばないことを表している.

いま数列

$$c_0, c_1, c_2, \ldots$$

が与えられたとき，これからつくられるべき級数

$$c_0+c_1x+c_2x^2+\cdots \tag{2.28}$$

を，この数列の**母関数 generating function** という．母関数は他にもあるので，それと区別するときには，(2.28) を**通常母関数**ともいう. (**z 変換**ともいう）
もっと一般に, n 個のもののうちから k 個のものを選び出す選び方 (組合せ) の個数は, 展開式

$$(1+x)^n = 1+nx+\cdots+\binom{n}{k}x^k+\cdots+x^n \tag{2.29}$$

の x^k の係数

$$\binom{n}{k} =_n C_k = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

で与えられる．したがって, $(1+x)^n$ は, 組合せを与える母関数である。（これを**（通常）係数子**ともいう.）

例題 3.1　５種類のものがあり，そのうち３種類が２個ずつあり，２種類が１個ずつあるとするとき，これらから，５個を選び出す方法は何通りあるか.
（解）a, b, c が２個ずつ，d, e が１個ずつとする．a を選ばない場合と，１個選ぶ場合と，２個選ぶ場合があるから，それを表すと

$$1 + a + a^2$$

b, c についても同じように，それぞれ $1 + b + b^2$，　$1 + c + c^2$ となる．また，d, e については，$1 + d$, $1 + e$ である．したがって母関数は

$$(1 + x + x^2)(1 + x + x^2)(1 + x + x^2)(1 + x)(1 + x) = (1 + x + x^2)^3(1 + x)^2$$

であるから，この式の展開式の x^5 の係数を求めればよい.
一般に, p 種類のもの２個ずつと，q 種類のもの１個ずつの中から k 個選ぶ選び方の個数は

$$\sum_{i=0}^{[k/2]} \binom{p}{i} \binom{p+q-i}{k-2i}$$

である．これは，$(1+x+x^2)^p$ から i 個の x^2 と，残り $p-i$ 個の因数 $(1+x+x^2)^{p-i}$ と q 個の因数 $(1+x)^q$ から $k-2i$ 個の x を選ぶ選び方の個数である．今の場合は $p = 3, q = 2, k = 5$ であるから，求める選び方は

$$\sum_{i=0}^{2} \binom{3}{i} \binom{3+2-i}{5-2i} = 22 \text{ 通り}$$

例題 3.2　n 個のものから重複を許して m 個選び出す選び方の総数を求めよ.
(解)　無制限に重複を許すことにすると，母関数は

$$\begin{aligned} f(x) &= (1 + x + x^2 + \cdots)^n = (\frac{1}{1-x})^n \\ &= \sum_{k=0}^{\infty} \frac{(-n)(-n-1)\cdots(-n-k+1)}{k!}(-x)^k \\ &= \sum_{k=0}^{\infty} \frac{n(n+1)\cdots(n+k-1)}{k!}x^k \end{aligned}$$

であるから求める数は x^m の係数

$$\binom{n+m-1}{m}$$

に等しい.（これは，2.1.5 の結果 (2.6) と一致する.）

例題 3.3　１円玉が１０個，５円玉が４個，１０円玉が３個あるとき，これらを使って１５円支払いたい．組合せはいくつあるか.
（解）この問題では，５円玉は１円玉を５個ひとまとめにしたものと考えることができる．そこで，１円玉を１つとることを x で表すならば，５円玉を１つとることは x^5 で表すことができる.

１円玉を選ぶ組合せの母関数は

$$1 + x + x^2 + \cdots + x^{10}$$

５円玉を選ぶ組合せの母関数は

$$1 + x^5 + x^{10} + \cdots + x^{20}$$

１０円玉を選ぶ組合せの母関数は

$$1 + x^{10} + x^{20} + x^{30}$$

であるから，この場合の母関数はこれらの積

$$(1 + x + x^2 + \cdots + x^{10})(1 + x^5 + x^{10} + x^{15} + x^{20})(1 + x^{10} + x^{20} + x^{30})$$

である．k 円を選ぶ方法の総数は, この母関数の展開式の x^k の係数である．$k = 15$ とすれば, ５通りである.

2.3.2　指数型母関数

数列 $\{c_k\}$ に対して

$$c_0 + c_1 \frac{1}{1!}x + c_2 \frac{1}{2!}x^2 + \cdots \tag{2.30}$$

を**指数型母関数** という.

$$(1+x)^n = 1 + \frac{{}_nP_1}{1!}x + \frac{{}_nP_2}{2!}x^2 + \cdots + \frac{{}_nP_k}{k!}x^k + \cdots + \frac{{}_nP_n}{n!}x^n \tag{2.31}$$

であるから，$(1+x)^n$ は，順列を表す指数型母関数である.

例題 3.4　0,1,2,3 の４つの数字を並べてできる数を４元数という．r 桁の４元数で，1,2,3 のどれもが少なくとも１回は現れるものの個数を求めよ．
(解)　これは，４種類のもののうち，３種類のものは必ず選ぶという条件のもとで r 個の順列を求めることと同じである．　数字 0 の計数子は

$$1+x+\frac{1}{2!}x^2+\frac{1}{3!}x^3+\cdots=e^x$$

である．数字 1 , 2, 3 の計数子は

$$x+\frac{1}{2!}x^2+\frac{1}{3!}x^3+\cdots=e^x-1$$

である．ゆえに，４種類の順列の母関数は

$$\begin{aligned} e^x(e^x-1)(e^x-1)(e^x-1) &= e^{4x}-3e^{3x}+3e^{2x}-e^x \\ &= \sum_{k=0}^{\infty}\frac{4^k-3\cdot 3^k+3\cdot 2^k-1}{k!}x^k \end{aligned}$$

したがって，求める数は, $4^r-3\cdot 3^r+3\cdot 2^r-1$ である．

2.3.3　分配の問題（続)

相異なるものの同種の部屋への分配

n 個の相異なるものを同種の k 個の部屋に, どの部屋にも少なくとも１つは入るように分配する仕方の総数は，第２種スターリング数を $S(n,k)$ である (2.1.6 節参照）. これをを母関数を用いて計算する．まず, n 個の相異なるものを k 個の相異なる部屋に，１つ以上ずつ分配する問題を考える．１つの部屋の指数型母関数は

$$x+\frac{1}{2!}x^2+\frac{1}{3!}x^3+\cdots=e^x-1$$

であるから, k 個の部屋に対する指数型母関数は

$$\begin{aligned} (e^x-1)^k &= \sum_{m=0}^{k}\binom{k}{m}(-1)^m e^{(k-m)x} \\ &= \sum_{m=0}^{k}\binom{k}{m}(-1)^m\sum_{r=0}^{\infty}\frac{1}{r!}(k-m)^r x^r \\ &= \sum_{r=0}^{\infty}\frac{1}{r!}x^r\sum_{m=0}^{k}\binom{k}{m}(-1)^m(k-m)^r \end{aligned}$$

したがって, 求める総数は $\dfrac{1}{n!}x^n$ の係数

$$\sum_{m=0}^{k}\binom{k}{m}(-1)^m(k-m)^n=\sum_{m=0}^{k}\binom{k}{m}(-1)^m m^n \tag{2.32}$$

に等しい.

部屋を区別しない場合は, この数を $k!$ で割ればよいから

$$S(n,k) = \frac{1}{k!}\sum_{m=0}^{k}\binom{k}{m}(-1)^m(k-m)^n \tag{2.33}$$

となる.

整数の分割（同種のものの同種の部屋への分割）　正の整数 k が与えられたとき，これをいくつかの正の整数の和として表す問題は，k 個の同種のものをいくつかのグループに分割する問題である．またこれは，同種の k 個のものを n 個の同種の部屋に分配する問題でもある．これを母関数で処理するには次のように考える．

まず，数 1 を k 個選ぶ方法は式

$$1 + x + x^2 + \cdots + x^n$$

における x^k の係数である．(もちろんそれは 1 に等しい.）しかし，この式の代わりに，無限級数

$$1 + x + x^2 + \cdots + x^n + \cdots$$

を用いても結果は同じであり，この方がすべての n に共通であるのことと，この式が $\dfrac{1}{1-x}$ と書けて簡単であるので母関数としてこの級数を用いる．

数 2 の母関数は

$$1 + x^2 + x^4 + \cdots + x^{2n} + \cdots = \frac{1}{1-x^2}$$

である．以下同様にして，数 m の母関数は

$$1 + x^m + x^{2m} + \cdots + x^{mn} + \cdots = \frac{1}{1-x^m}$$

となる．したがって，k を分割する問題の母関数は

$$f(x) = \frac{1}{(1-x)(1-x^2)\cdots(1-x^{mn})\cdots}$$

であり，m 以下の数を用いて分割する問題の母関数は

$$f(x) = \frac{1}{(1-x)(1-x^2)\cdots(1-x^{mn})}$$

である．たとえば，3 以下の整数の和に分ける母関数は

$$\frac{1}{(1-x)(1-x^2)(1-x^3)} = 1 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 7x^6 + \cdots$$

から，6 を 3 以下の整数に分割する方法は 7 ($= x^6$ の係数) 通りである.

例題 3.5 n を相異なる整数の和で表す仕方の総数は，n を奇数の和に表す仕方の総数に等しいことを示せ．
(解）n を相異なる正の整数の和で表すことの母関数は

$$\begin{aligned}(1+x)(1+x^2)(1+x^3)\cdots(1+x^m)& \\ &= \frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\cdot\frac{1-x^8}{1-x^4}\cdots \\ &= \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots}\end{aligned}$$

となるが，最後の式は奇数だけで表す母関数である．

例題 3.6 すべての正の整数は，２進法でただ１通りに表されることを示せ．
(解）これは，2^r の形の整数の和として表す仕方の総数を求める問題と同じである．その母関数は

$$f(x) = (1+x)(1+x^2)(1+x^4)(1+x^8)\cdots$$

である．この式の 1 の係数は 1 である．$r>1$ に対する x^r の係数を調べるため $(1-x)f(x)$ を考える．

$$\begin{aligned}(1-x)f(x) &= (1-x^2)(1+x^2)(1+x^4)(1+x^8)\cdots \\ &= (1-x^4)(1+x^4)(1+x^8)\cdots \\ &= (1-x^8)(1-x^8)(1-x^{16})\cdots \\ &= \cdots\end{aligned}$$

であるから $r>1$ に対する x^r の係数はすべて 0 で，結局

$$(1-x)f(x) = 1$$

$$f(x) = \frac{1}{1-x} = 1 + x + x^2 + \cdots + x^n\cdots$$

となるから，$f(x)$ における x^r の係数はすべて 1 である．

2.4　漸化式

2.4.1　定数係数線形差分方程式（漸化式）

$r+1$ 個の定数 $p_0, p_1, \cdots, p_r$ と，数列 $\{f(n)\}$ が与えられたとき，

$$p_0 a_n + p_1 a_{n-1} + \cdots + p_r a_{n-r} = f(n) \tag{2.34}$$

の形の式を（r **次の定数係数線形）漸化式 recurence formula** という．この式を満たす数列 $\{a_n\}$ を求めるという問題を考えるときは, これを **差分方程式 difference equation** といい，それを満たす数列 $\{a_n\}$ を**解 solution** という．最初の r 個の $a_0, a_1, \cdots, a_{r-1}$ の値を**初期条件**という．次のことが成り立つ.

任意の初期条件に対して，方程式 (2.34) の解がただ 1 つ存在する.

2.4.2　斉次線形差分方程式

とくに，$f(n) = 0$ の場合

$$p_0 a_n + p_1 a_{n-1} + \cdots + p_r a_{n-r} = 0 \tag{2.35}$$

を**斉次線形差分方程式**という．これらの解に対しては次のことが成り立つ

$\{a_n^{(1)}\}, \cdots, \{a_n^{(m)}\}$ が (3.35) の解であるとき,

$$b_n = c_1 a_n^{(1)} + \cdots + c_m a_n^{(m)}$$

とおくと，$\{b_n\}$ も (3.35) の解である.（**重ね合せの原理 principle of superposition**）

(2.34) の一般解 = (2.35) の一般解 + (2.34) の特解

$$p_0 \lambda^r + p_1 \lambda^{r-1} + \cdots p_r = 0 \tag{2.36}$$

を (2.35) に付随する**特性方程式**という.

λ が (2.36) の解であれば,

$$a_n = A\lambda^n \tag{2.37}$$

とおくと, $\{a_n\}$ は (2.35) の解である.

もし，$\lambda_1, \cdots, \lambda_r$ が (2.36) の相異なる実数解ならば

$$A_1\lambda_1^n + \cdots + A_r\lambda_r^n \tag{2.38}$$

とおくと，$\{a_n\}$ は (2.35) の解である．$A_1, .., A_r$ は初期条件によって定まる.

例題 4.1 Fibonatti の数列 $\{a_n\}$ は

$$a_n = a_{n-1} + a_{n-2}, \qquad a_0 = 0, \quad a_1 = 1$$

によって定義される数列である.
(解) 特性方程式は $\lambda^2 - \lambda - 1 = 0$ である．これを解いて 2 実解

$$\lambda_1 = \frac{1+\sqrt{5}}{2}, \qquad \lambda_2 = \frac{1-\sqrt{5}}{2}$$

が得られ，一般解は $A_1\lambda_1^n + A_2\lambda_2^n$ で, 境界条件 $a_0 = 0, \ \ a_1 = 1$ より A_1, A_2 を決定すると

$$A_1 = \frac{1}{\sqrt{5}}, \qquad A_2 = -\frac{1}{\sqrt{5}}$$

であるから

$$a_n = \frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \frac{1}{\sqrt{5}}\Big(\frac{1-\sqrt{5}}{2}\Big)^n$$

が得られる.

例 4.2　（ハノイの塔）大きさの異なる穴のあいた円板が n 枚あって, 大きさの順に 1 本の棒に通されている．他に 2 本の棒がある．　これらの円板を他の 1 本の棒に移し替えたい．1 回に 1 枚の円板を動かすとして, 何回の操作で全部移し替えることができるか．
3 本の棒は何回利用してもよいが, 操作の途中で, 大きい円板を小さい円板の上にのせてはならない．
(解）必要な回数を a_n とする．あきらかに $a_1 = 1$ である．いま $n-1$ 枚の円板を 1 本の棒に移し終わったとすると, これまでにかけた手数は a_{n-1} である．最後の 1 枚を残った棒に移す手数 1 回と, $n-1$ 枚の円板をその上に移す手数 a_{n-1} が必要であるから漸化式は
$(*)$　　$a_n = 2a_{n-1} + 1$
となる．　斉次方程式 $a_n = 2a_{n-1}$ の特性方程式は $\alpha - 2 = 0$ であるからその一般解は $A2^n$．また,(*) の特解として -1 があるから (*) の一般解は $\alpha_n = A2^n - 1$ である．境界条件　$a_1 = 1$ により $a_n = 2^n - 1$ が得られる．
（$n = 64$ のとき, 1 回に 1 秒かかるものとすると, 全部に要する時間は　$2^{64} - 1 \approx$ 5850 億年）

フィボナッティ数について　通称 Fibonacci (Filus Bonacci ボナッティの息子）本名 Leonardo da Pisa (ピサのレオナルド）16-17 世紀の人.「算術書」(Bibre Abacci) という著書があり, 2 世紀の間ヨーロッパで広く読まれた．その中に，次の問題がある．1 つがいの兎がいて, 1 月毎に 1 つがいの兎を生む．生まれた兎は 2 月目から 1 つがいの兎を生む．nヶ月目には兎は何匹になっているか。この答えがフィボナッティ数である．約 400 年後 フランスの数学愛好家 リュカ Edward Lucas がこれを研究し有名になった．自然界の色々な現象と関係があり, 世界中にフィボナッティ数を研究する数学愛好家がたくさんいて,「フィボナッティ協会」というのがある．
フィボナッティ数列 $\{a_n\}$ について多くのことが知られている．たとえば
(1) $a_{n+m} = a_{n-1}a_m + a_n a_{m+1}$　$(n \geq 1,\ m \geq 0)$
(2) $a_n | a_{mn}$　$(m, n \geq 1)$
(3) a_n が素数ならば n は素数 $(n \neq 4)$
(4) a_n と a_{n+1} は互いに素
(5) $m \geqq n \geqq 1$ とする．$a_n | a_m$ ならば $n | m$.
(6) $\lim_{n\to\infty} a_{n+1}/a_n = \dfrac{\sqrt{5}-1}{2}$(黄金比)

2.4.3　母関数 (Z 変換）による解法

例題 4.3　漸化式

$$a_{n+2} - 5a_{n+1} + 6a_n = 5^n \qquad a_0 = 0,\ \ a_1 = 1$$

の解を求めよ.
(解) 漸化式の両辺に x^{n+2} $(|x|<5)$ をかけて 0 から ∞ まで加えると,

$$\sum_{n=0}^{\infty} a_{n+2}x^{n+2} - 5x\sum_{n=0}^{\infty} a_{n+1}x^{n+1} + 6x^2\sum_{n=0}^{\infty} a_n x^n = x^2\sum_{n=0}^{\infty} 5^n x^n$$

$$\sum_{n=2}^{\infty} a_n x^n - 5x\sum_{n=1}^{\infty} a_n x^n + 6x^2\sum_{n=0}^{\infty} a_n x^n = x^2\sum_{n=0}^{\infty} 5^n x^n$$

$\{a_n\}$ の母関数を $A(x)$ とおく：

$$A(x) \equiv \sum_{n=0}^{\infty} a_n x^n (= \sum_{n=1}^{\infty} a_n x^n)$$

上の式は

$$A(x) - a_1 x - 5xA(x) + 6x^2 A(x) = x^2\sum_{n=0}^{\infty} 5^n x^n$$

となる. 整理して部分分数分解すると

$$A(x) = -\frac{2}{3}\frac{1}{1-2x} + \frac{1}{2}\frac{1}{1-3x} + \frac{1}{6}\frac{1}{1-5x} = -\frac{2}{3}\sum_{n=0}^{\infty} 2^n x^n + \frac{1}{2}\sum_{n=0}^{\infty} 3^n x^n + \frac{1}{6}\sum_{n=0}^{\infty} 5^n x^n$$

が得られる. したがって, 解は次のようになる.

$$a_n = -\frac{2}{3}2^n + \frac{1}{2}3^n + \frac{1}{6}5^n$$

この解法と, 前節で述べたことを併せて考えると, 母関数による漸化式の解法と, ラプラス変換による微分方程式の解法との類似に想到する. そこで, 母関数のことを離散的ラプラス変換あるいは Z変換と名付ける. ラプラス変換とその微分方程式への応用については付録 2 を参照.

2.5　数え上げ

2.5.1　Burnside の定理

G は，有限集合 Ω の置換群であるとする．　Ω の元 a, b に対して，ある $g \in G$ があって，$b = g(a)$ となるとき，a と b とは同値であるということにすると，Ω は同値類に分割される．この同値類の数を数えるという問題を考える．

例として，黒色と白色の玉合, 計６個の玉を紐に通して出来るネックレースは幾つ出来るかという問題を考える．　ネックレースを，下の図のように, 円周の６つの点に黒い印と白い印をつけたものとものと考え，玉を置く場所に番号をつける．

図 2.1:

図の (a),(b),(c) はネックレースとしては同じである．(a) の番号に対して置換

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (1,2,3,4,5,6)$$

を行うと (b) が得られる．これは回転である．また (a) の番号に置換

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1,6)(2,5)(3,4)$$

を行うと (c) が得られる．これは裏返しである．

番号のついたネックレースの集合を Ω とし，回転および裏返しからなる置換群（６次の２面体群）を G とする．これらの置換によって同値なものは，ネックレースとしては同じものと考えられるから，ネックレースの個数は，G による同値類の個数に等しい．

一般にこのような問題の解は，次の定理から得られる．

定理 2.5.1 (Burnside の定理) G による Ω の同値類の個数は

$$\frac{1}{|G|}\sum_{g\in G}\psi(g) \tag{2.39}$$

ここで，$\psi(g)$ は，置換 g によって不変な Ω の元の個数である．

（証明）Ω の元 x に対して，x を不変にするような G の元の個数を $\eta(x)$ で表すと

$$\sum_{x\in\Omega}\eta(x)=\sum_{g\in G}\psi(g)$$

が成り立つ．これらの量が，集合

$$\{(x,g): x\in\Omega,\ g\in G,\ g(x)=x\}$$

の大きさに等しいからである． 定理を証明するには, Ω の同値類の個数が

$$\frac{1}{|G|}\sum_{x\in\Omega}\eta(x)$$

に等しいことを示せばよい.

いま，$x, y\in G$ に対して，x を y に写す置換全部の集合を $E_{x,y}$ とする：

$$E_{x,y}=\{g\in G: g(x)=y\}$$

x と y が同値であるときは，$E_{xy}\neq$ である．とくに $E_{xx}=\pi_x$ と書く：

$$\pi_x=\{g\in G: g(x)=x\}$$

$|\pi_x|=\eta(x)$ である.
x と y が同値として，$g\in E_{xy}$ を1つとる．$g'\in\pi_x$ ならば $gg'\in E_{xy}$. 逆に $h\in E_{xy}$ ならば $g^{-1}h\in\pi_x$, よって $h\in g\pi_x$ となるから，$g\pi_x=E_{xy}$ となる．したがって，$|E_{xy}|=|g\pi_x|=|\pi_x|=\eta(x)$ が得られる.

いま，x_1 を含む同値類を

$$[x_1]=\{x_1,x_2,..,x_m\}$$

とするとき，すべての置換は，x_1 を x_1 に写す置換，x_1 を　x_2 に写す置換，.., x_1 を x_m に写す置換と分類され，その各々の個数はすべて $\eta(x)$ に等しいから

$$|G|=m\eta(x)$$

が成り立つ. 同様の考察を $x_2,..,x_m$ に行って,

$$\eta(x_1)=\eta(x_2)=\cdots=\eta(x_m)=\frac{|G|}{m}$$

が得られる. したがって

$$\eta(x_1) + \cdots + \eta(x_m) = |G|$$

が成り立つ. このことが各同値類について成り立つから

$$\sum_{x\in\Omega} \eta(x) = |G| \times (\text{同値類の個数})$$

となる. □

上のネックレースの例では, G は次の１２個の元からなる.

$$\begin{array}{ll} e = (1)(2)(3)(4)(5)(6) & \beta = (1,6)(2,5)(3,4) \\ \alpha = (1,2,3,4,5,6) & \alpha\beta = (1,5)(2,4)(3,6) \\ \alpha^2 = (1,3,5)(2,4,6) & \alpha^2\beta = (1,5)(2,4)(3)(6) \\ \alpha^3 = (1,4)(2,5)(3,6) & \alpha^3\beta = (1,3)(2)(4,6)(5) \\ \alpha^4 = (1,5,3)(2,6,4) & \alpha^4\beta = (1,2)(3,6)(4,5) \\ \alpha^5 = (1,6,5,4,3,2) & \alpha^5\beta = (1)(2,6)(2,5)(4) \end{array}$$

このうち, α , α^3, α^5 β $\alpha\beta$ および $\alpha^4\beta$ によって不変なネックレースはすべての玉が同一色のものであるか, または４個が同色のものである, この問題では, 同色のものは３個ずつであるから.

$$\psi(\alpha) = \psi(\alpha^3) = \psi(\alpha^5) = \psi(\beta) = \psi(\alpha^2\beta) = \psi(\alpha^4\beta) = 0$$

となる. その他のものは

$$\psi(e) = \binom{6}{3} = 20, \quad \psi(\alpha^2) = \psi(\alpha^4) = 2, \quad \psi(\alpha^2\beta) = \psi(\alpha^3\beta) = \psi(\alpha^5\beta) = 4$$

であるから, Burnside の定理により, ネックレースの個数は

$$\frac{\sum_{g\in G} \psi(g)}{|G|} = \frac{36}{12} = 3$$

である.

2.5.2　ポリアの定理

再び６個の玉からなるネックレースを考える. 前節では, ３個の黒玉と３個の白玉の場合を考えたが, ここでは, その他の場合も同時に処理できるもっと能率のよい方法を述べる.　今度は, 番号のついたネックレースの集合を Ω とする. 置換の１つ, たとえば

$$g = \alpha^2\beta = (1,5)(2,4)(3)(6)$$

によって不変な Ω の元の集合を Ω_g とすると, Ω_g の元は, (1) と (5) の位置にある玉の色が同じものなければならない. いま黒玉を x, 白玉を y で表すことにすると, (1) と (5) では, x を 2 個とるか, y を 2 個とるかであるからそれを表す母関数は x^2+y^2 である. (2,4) についても同じである. また, (3) と (6) については, 黒玉 1 つまたは白玉 1 個であるから $x+y$ である. したがって, Ω_g の元を表す母関数は

$$(x^2+y^2)(x^2+y^2)(x+y)(x+y) = (x^6+y^6)+(x^5y+xy^5)+(x^4y^2+x^4y^2)+4x^3y^3$$

である. このことから, 黒玉 3 個白玉 3 個の番号のついたネックレースのうち, g によって不変なものの個数は 4 個あることがわかる.

このような母関数を g の**環指標 cycle index** といい, $C_g(x,y)$ で表す. 一般に, x と y の 2 種類からなる番号のついたものの集合 Ω に, 置換群 G が働いているとする. このとき次のことが成り立つ.

定理 2.5.2 (Polya の定理) すべての $g \in G$ の環指標の平均, すなわち

$$\frac{\sum_{g\in G} C_g(x,y)}{|G|} \tag{2.40}$$

の展開式において, $x^k y^{n-k}$ の係数は, k 個の x と $n-k$ 個の y を含むものの G による同値類の個数を表す.

上の例でいうと, この平均は

$$\frac{1}{12}\left\{(x+y)^6+3(x+y)^2(x^2+y^2)^2+4(x^2+y^2)^3+2(x^3+y^3)^2+2(x^6+y^6)\right\}$$
$$= y^6+xy^5+3x^2y^4+3x^3y^3+3x^4y^2+x^5y+x^6$$

となる. これから, 白玉 3 個黒玉 3 個のネックレースは 3 個あることが判るが, 同時に, 白玉 2 個、黒玉四個のものが 3 個あることも判る. 他の組合せについても同様である.

今度は, 黒玉と白玉と赤玉合計 6 つの場合を考える. 上と同じく

$$g = \alpha\beta = (1,5)(2,4)(3)(6)$$

について考えると, 母関数は

$$C_g(x,y,z) = (x+y+z)^2(x^2+y^2+z^2)^2$$

となる. Polya の定理によると

$$\sum_{g\in G} C_g(x,y,z)/|G|$$

の $x^i y^j z^k$ の係数が, 黒玉 i 個, 白玉 j 個, 赤玉 k 個のネックレースの個数を与える. たとえば, 黒玉 2 個, 白玉 2 個、赤玉 2 個のネックレースの個数は, $x^2y^2z^2$ の係数 11 に等しい.

2.5.3 包除原理 principle of inclusion and exclusion

有限集合 E の各元 x に実数の重み $m(x)$ が与えられているとする. $A \subset E$ に対して

$$m(A) = \sum_{x \in A} m(x) \tag{2.41}$$

と定義する. ただし, $m(\phi) = 0$ とする. とくに

$$m(x) = 1, \quad x \in E$$

のときは $m(A)$ は A の元の個数 $|A|$ に等しい.

E の部分集合 $A_1, .., A_n$ と $N = \{1, \ldots, n\}$ の部分集合 I に対して

$$A_I = \cap_{\imath \in I} A_i \qquad A = E \tag{2.42}$$

と書く.

篩の公式

$$m\left(\cup_{I \subset N} A_I\right) = \sum_{\neq I \subset N} (-1)^{|I|-1} m(A_I) \tag{2.43}$$

が成り立つ. とくに

$$|\cup_{I \subset N} A_I| = \sum_{\neq I \subset N} (-1)^{|I|-1} |A_I| \tag{2.44}$$

となる. 補集合をとると次の**包除公式**が得られる.

$$|E - \cup_{I \subset N} A_I| = \sum_{\neq I \subset N} (-1)^{|I|} |A_I| \tag{2.45}$$

例 5.1 1 から 250 までの整数の中に 2,3,5,7 のどれによっても割りきれないものはいくつあるか.

（解）2,3,5,7 を x_1, x_2, x_3, x_4 で表し, x_i で割りきれるということを A_i で, x_i, x_j で割りきれるということを A_{ij} で表し, ... とすると,

$$|A_1| = 125, |A_2| = 83, |A_3| = 50, |A_4| = 35, |A_{12}| = 41, |A_{13}| = 25, |A_{14}| = 17,$$

$$|A_{23}| = 16, |A_{24}| = 11, |A_{34}| = 7$$

$$|A_{123}| = 8, |A_{124}| = 5, |A_{134}| = 3, |A_{234}| = 2, |A_{1234}| = 1$$

であるから, 求める個数は

$$|E - \cup A_I| = 250 - (125 + 83 + 50 + 35) + (41 + 25 + 17 + 16 + 11 + 7) - (8 + 5 + 3 + 2) + 1 = 57$$

2.5.4　鳩の巣原理 pegionhole principle

「$n+1$ 羽の鳩が n 個の巣に入れば, 少なくとも 1 つの巣には 2 羽以上の鳩が入る」というのである.

例 5.2　5 つの器具の間に何本かの結線があるとき，どれか 2 つは，器具から出る線の本数が等しいことを示せ.

（解）1 つの器具から出る線の本数は 0, 1, 2, 3, 4 本の 5 種類ある．しかし，4 本の線が出る器具があることと，本数が 0 の器具があることとは両立しない．したがって，実際に起こる本数の種類はつねに 4 種類以下である．5 つのものを 4 種類に分ければ必ずどれか 2 つは同じ種類のものである.

演 習 2

1. 2 項係数の性質 (1) - (12) を証明せよ.

2. ２項分布 $b(r;N,p)$ の分散と平均を計算せよ.

3. n 個のものから偶数個取り出す選び方の総数と，奇数個取り出す選び方の総数は等しいことを示せ.

4. $(10!)!$ は $10^{9!}$ で割りきれることを示せ.（10 個ずつ，9!種類のものの順列を求める：もっと一般な命題は？）.

5. $2n$ 個のもののうち n 個のものが同種である。これら 2n 個のものから n 個選ぶ選び方の総数を求めよ.

6. 円周上に６つの点があるとき，２点を結んでできる線分は何本あるか．また，３点を結んでできる３角形はいくあるか.

7. ７人の男子生徒と５人の女子生徒のうちから、男女２人ずつの代表を選び出す方法は何通りあるか

8. 赤，青，黄色の三色の玉を６個選び出す方法はいく通りあるか.

9. 0 と 1 からなる数を２元数列という．n 桁の２元数のうち, 0 を偶数個含むものはいくつあるか.

10. 三桁までの数のうち，各桁の数字の合計が１０となるものは全部でいくつあるか.

11. ４種類のものを６個選び出す方法は何通りあるか.

12. １０個の赤球と５個の白球を５人に分配する方法は何通りあるか.

13. r 桁の４元数列で，0 を偶数個含むものは幾つあるか．また， 0 と 1 を偶数個含むものは幾つあるか.

(hint: 0 の指数型母関数は $1+\dfrac{x^2}{2!}+\dfrac{x^4}{4!}+\cdots$)

14. ４桁の電話番号は何通り作れるか．４桁の電話番号のうち４つの数が相異なるものはいくつあるか.

15. 赤球１０個，白球１２個，青球１５個のうちから，１４個を選ぶ方法は何通りあるか．ただし，赤球は少なくとも４個，白球は少なくとも３個，青球は少なくとも５個以上選ぶものとする.

16. $\dfrac{1}{(1-x)^2}$と$\dfrac{1}{(1-x)^3}$ はどんな数列の母関数か.

17. 平面上に１つの円と n 本の直線がある．３本の直線が１点で交わることはなく, また, 交点はすべて円の内部にあるとする.
このとき, 円の内部は直線によって、いくつの領域に分けられるか.

18. 例題 4.1, と例題 4.2 を母関数の方法で解け.

19. アルファベット $\{a,b,c\}$ からつくられる長さ n の単語で, a が偶数回現れるような単語の数が $(3^n+1)/2$ であることを示せ

20. $x_1+\cdots+x_6=20 \quad (2 \leqq x_i \leqq 8)$ の整数解は何通りあるか.（２０個の同種のものを６個の異なった部屋に分配するとき，どの部屋にも２個以上８個までとする方法の個数）

21. ３つの林檎，４つの柿，５つの梨を，２つの箱A，Bに６つずつ入れる方法は何通りか.

22. ４つの文字ＭＡＴＨから重複を許して５つの文字を選ぶとき，Aは少なくとも１つ，ＴとＨは高々１つにする方法は何通りあるか.

23. 正の整数は，１０進法でただ１通りに表されることを示せ.

24. n 本の直線によって平面はいくつの領域に分割されるか．ただし，どの２本の直線も平行でなく，またどの３本も１点で交わらないものとする.

25. 漸化式 $a_n = 3a_{n-1} + 5$ を次の初期条件で解け.
(1) $a_0 = 2$ (2) $a_0 = 1$

26. 漸化式 $a_n = a_{n-1} + 2(n-1), \quad a_0 = 1$ を解け.

27. n 個の円が互いに必ず２点で交わり，しかもどの３個の円も１点で交わることがないとすると、これらの円は平面をいくつの領域に分割するか

28. １００の学生のうち，英語のクラスに出席しているものは８０人，ドイツ語のクラスには７５人，両方のクラスに出るものは６０人であるという．どちらにも出席しない学生は何人か.

29. ７０以下の自然数で，７０と公約数をもたないものはいくつあるか.

30. パーティーを開くと，その中のだれか２人は，知り合いの数が等しい事を示せ.

31. ７つの自然数があると，その中どれか２つの和か差が 10 で割りきれることを示せ.

付　　録

1. 置換

$\Omega = \{1, 2, .., n\}$ から Ω への 1 対 1 写像 を n **次の置換**という. n 次の置換のつくる群を n **次対称群**といい，S_n で表す.

n 次の置換 P において, $1, 2, \ldots n$ のそれぞれに対応する数を $p_1, p_2, \ldots p_n$ とするとき, 写像 P を

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}$$

で表すのが普通であるが，対応さえ同じであれば,

$$\begin{pmatrix} s_1 & s_2 & \ldots & s_n \\ t_1 & t_2 & \ldots & t_n \end{pmatrix}$$

などと書いてもかまわない．これは $1.2. \ldots n$ の順列と考えられるから，S_n の位数は $n!$ である．2 つの置換

$$P = \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}, \qquad Q = \begin{pmatrix} 1 & 2 & \ldots & n \\ q_1 & q_2 & \ldots & q_n \end{pmatrix}$$

があるとき，P を

$$P = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \ldots & r_n \end{pmatrix}$$

と書きなおして

$$PQ = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \ldots & r_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \ldots & n \\ q_1 & q_2 & \ldots & q_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ r_1 & r_2 & \ldots & r_n \end{pmatrix}$$

によって積 PQ が定義される．たとえば

$$\begin{aligned} &\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} \end{aligned}$$

という具合である.

任意の置換 P に対して

$$\begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

を P の逆置換といい，P^{-1} で表す．また，置換

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

を I で表す．すべての置換 P に対して次のことが成り立つ．

(1) $PI = IP = P$

(2) $PP^{-1} = P^{-1}P = I$

置換 P において, $i < j$ でかつ $p_j < p_i$ となる $i,\ j$ の組合せを**転位**という．互換 (i, j) には $|i - j| - 1$ 個の転位がある．

文字 $x_1, \dots, x_n$ の式

$$\Delta = \Delta(x_1, .., x_n) = \Pi_{i<j}(x_i - x_j)$$

を**差積** という．$\Delta_P = \Delta(x_{p_1}, .., x_{p_n}$ とおく．P に含まれる転位の個数を r とすると

$$\Delta_P = (-1)^r \Delta$$

置換 P を互換の積で表すとき，互換の個数が偶数であるか奇数であるかは P によって定まる．偶数のときは**偶置換**，奇数のときは**奇置換**という．